

Census Employee Handbook for Enumerators and Recruiting Assistants

2020 Census Peak Operations



U.S. Department of Commerce
Economics and Statistics Administration
U.S. Census Bureau

U.S. Department of Commerce
Economics and Statistics Administration
U.S. Census Bureau

This document contains no Title 13 data or Personally Identifiable Information (PII). Examples do not contain real names, real addresses, or other real data.

This Page Intentionally Left Blank

Table of Contents

Chapter 1: Census Employment	1-1
Topic 1: Vision and Mission Statements	1-1
Topic 2: Organizational Structure Charts	1-2
Chapter 2: You and the Public	2-1
Topic 1: Identification Card	2-1
Topic 2: Face Coverings	2-2
Topic 3: Confidentiality	2-4
Topic 4: False Statements and Information	2-10
Topic 5: Political Activity	2-11
Topic 6: Outside Activities and Conflicts of Interest	2-13
Topic 7: Post-Employment Restrictions Under 18 U.S.C. 207	2-15
Topic 8: Summary of Ethics Rules	2-16
Chapter 3: Personnel and Payroll	3-1
Topic 1: Your Appointment	3-1
Topic 2: Your Salary	3-7
Topic 3: Your Job Activities and Authorized Hours	3-13
Topic 4: Reimbursable Expenses	3-16
Topic 5: How To Complete Your Paper Daily Payroll Form	3-19
Topic 6: How To Complete Your Electronic Daily Payroll Form	3-21
Topic 7: Submission of Paper Payroll Documents	3-30
Topic 8: Disallowances and/or Reclaims for Paper Payroll Forms	3-31
Topic 9: Fraudulent Claims Against the United States	3-32
Topic 10: Designation of Beneficiary for Unpaid Compensation of Deceased Civilian Employees	3-33
Topic 11: Employment Resolution Contact	3-34
Chapter 4: Travel Expenses	4-1
Topic 1: General	4-1
Topic 2: Per Diem Expenses	4-3
Chapter 5: Personal Safety and Security	5-1
Topic 1: Coverage	5-1

Topic 2: Safety	5-3
Topic 3: Vehicular Accidents.....	5-8
Topic 4: Personal Injuries.....	5-11
Topic 5: Assaults.....	5-15
Topic 6: Accident/Injury/Property Damage Forms Chart	5-17
Topic 7: Liability and Accountability for all Title 13 Materials and Data.....	5-21
Chapter 6: Personal Property and Damage Claims	6-1
Topic 1: Claim Information.....	6-1
Topic 2: Permissible Claims	6-2
Topic 3: Making A Personal Property Claim.....	6-4
Chapter 7: Employee Relations	7-1
Topic 1: Equal Employment Opportunity (EEO)	7-1
Topic 2: Sexual Harassment.....	7-3
Topic 3: Fraud, Waste, and Abuse.....	7-4
Topic 4: Pursuing Complaints.....	7-6
Topic 5: ACO Administrative Grievance Procedure	7-7
Topic 6: Important Contact Information	7-9
Appendix A: Forms for Employee Use.....	A-1
Appendix B: Rules and Regulations Governing Conduct on Federal Property	B-1
Appendix C: Records Management Training	C-1
Appendix D: 2019 U.S. Census Bureau Data Stewardship and Information Technology (IT) Security Awareness and No Fear Training	D-1

Chapter 1: Census Employment

Topic 1: Vision and Mission Statements

The Census Bureau is frequently referred to as the “Fact Finder for the Nation.”

We hire thousands of temporary employees, like you, to collect decennial statistics of population and housing, as well as social and economic data for use by the Federal Government, businesses and industries, and various other public and private organizations. The Census Bureau will be the supplier of choice for social and economic statistics important to the United States, and a leader among statistical agencies of the world.

Census Bureau’s Vision

“Quality Data - at the Right Time, for the Best Value”

Quality Data

We will collect accurate and complete data and achieve the highest possible response rate.

At the Right Time

We will guarantee the delivery of data that meets or exceeds our customer’s timing needs.

For the Best Value

We will provide the highest quality data for the lowest cost possible through continuous improvement.

Census Bureau’s Mission

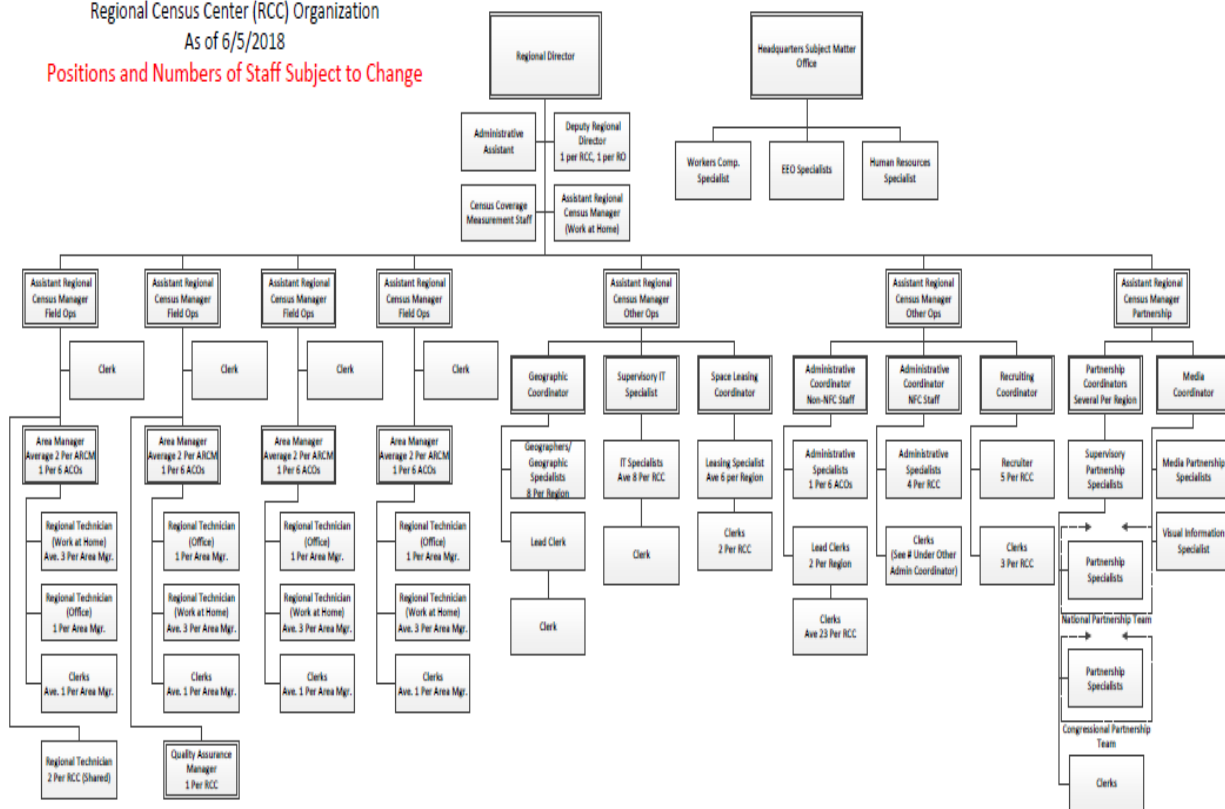
The Census Bureau serves as the leading source of quality data about the Nation’s people and economy. We honor privacy, protect confidentiality, share our expertise globally, and conduct our work openly. We are guided on this mission by our strong and capable workforce, our readiness to innovate, and our abiding commitment to our customers.

Your Mission

As a Census Bureau employee, your mission is to collect data through either personal interviews or telephone interviews. Your participation in this endeavor will play a major role in deciding this great nation’s future.

Topic 2: Organizational Structure Charts

2020 Census
Regional Census Center (RCC) Organization
As of 6/5/2018
Positions and Numbers of Staff Subject to Change

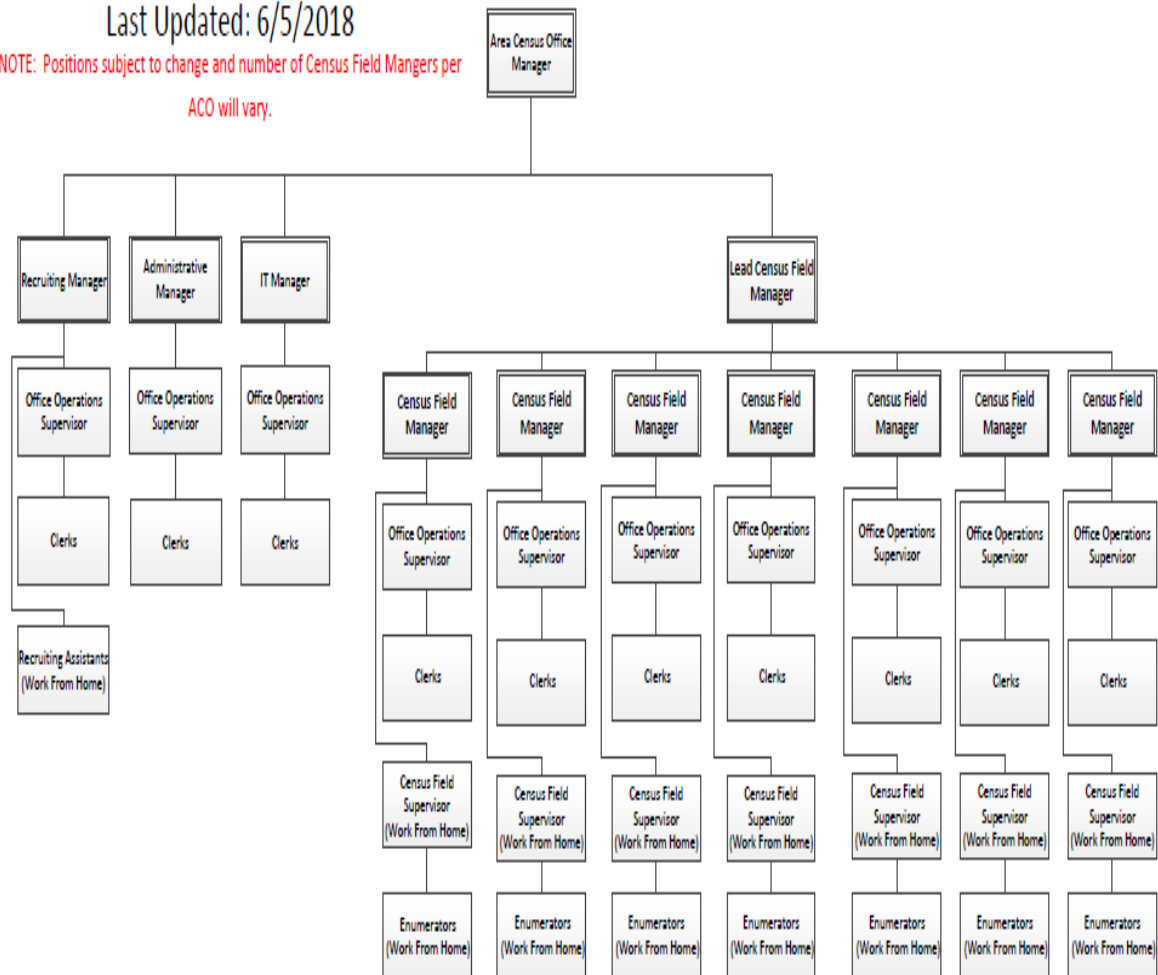


2020 Census Area Census Office Organization

Last Updated: 6/5/2018

NOTE: Positions subject to change and number of Census Field Managers per

ACO will vary.





The United States Census Bureau



the supplier of social and economic data,



about its people,



for its people.

“Quality Data – at the Right Time, for the Best Value”

-- Census Bureau’s Vision

Chapter 2: You and the Public

Topic 1: Identification Card

**Wear your official
picture ID card**

At the time you were appointed, you were issued an official Census picture identification card with the expiration date of your appointment. Wear this card whenever you are working for the Census Bureau.

**Reporting stolen or lost
ID cards**

If your ID card is lost or stolen, call the Decennial Service Center at (855) 236-2020 option #1. You also need to submit a written statement to your supervisor explaining the facts surrounding the loss and your efforts to recover the card. Your supervisor will arrange for you to receive another ID card. Further instructions can be found in Chapter 5, Topic 7 of this manual.

**What to do with your
ID card when you
separate**

When your appointment ends, or if you resign, turn in your ID card to your supervisor along with any remaining work assignments and other census materials and equipment.

Failure to turn in your ID card, and other census materials, can delay receipt of your final paycheck.

Topic 2: Face Covering

Face Covering is Mandatory

As part of our ongoing efforts to keep employees and the general public safe, face coverings are now mandatory. Field Division requires that all employees wear face coverings that cover your nose and mouth while interacting with fellow employees, the public, and while conducting field operations. According to the CDC, face coverings help decrease the spread of COVID-19. If you have any concerns regarding your ability to comply with this directive, please contact with your immediate supervisor as soon as possible.

The requirement for face coverings does not supersede or substitute the previously established COVID-19 guidance that you received. Therefore, you are required to wear face coverings if you are not 6 feet away from others, avoid contact with people who are sick, and wash your hands often with soap and water or hand sanitizer. A failure to comply with the directive to wear face coverings and/or adhere to any other established COVID-19 guidance may result in administrative action, up to and including, termination.

Additional Guidelines

- For your safety, employees should remove their face covering while driving between assignments.
- By wearing a face covering, you are letting all staff around you and the American public know you “have them covered” and this personal protective item represents one of the most effective ways to protect each other.

Face Mask Graphic

Below is the face mask graphic which provides important information on how to properly wear and remove a face mask as well as some helpful health and sanitization tips while using a face mask.

How to Wear a Cloth Face Mask

Here are a few tips for wearing and removing a cloth mask:

- Wash or sanitize your hands before wearing.
- Mask should cover the nose, mouth, and chin.
- Tie it behind your head or use the ear loops and ensure it is snug.
- Avoid touching the mask while wearing.
- If the mask is touched, wash or sanitize your hands immediately.
- While untying, avoid touching the front of the mask.
- Wash your hands immediately after removing.
- Regularly launder your mask. You can also launder it with your other clothes.

Finally, here are a few face mask precautions:

- Do not put masks on anyone who has trouble breathing, is unconscious, or otherwise unable to remove the mask without assistance.
- Do not use face masks as a substitute for social distancing.



For the latest updates on the COVID-19 pandemic, check the **Centers for Disease Control and Prevention Web site** and [mayoclinic.org](https://www.mayoclinic.org).



U.S. Department of Commerce
U.S. CENSUS BUREAU
[census.gov](https://www.census.gov)

Topic 3: Confidentiality

Confidential Information

Your position with the Census Bureau has important responsibilities regarding the confidentiality of data collected. Title 13, United States Code, requires that data from individuals and establishments be used only as statistical totals. This means identification of individuals or establishments must never occur and only sworn Census Bureau employees may examine the information you collect. Do not release any data to persons not employed by the Census Bureau including family members.

The Census Bureau's reputation for nondisclosure of data is a major factor in obtaining respondent cooperation.

General Guidelines

- Only government and Special Sworn Status (SSS) employees should handle PII data
- Material containing PII must be safeguarded at all times. At no time should PII be left unsecured.
- All PII that is shipped must be double wrapped, labeled as PII, and tracked
- PII that is sent via email must be encrypted
- Any breach must be reported within one hour of discover

Definition: 'census-confidential'

The term 'census-confidential' means all information the Census Bureau collects is legally prohibited from being disclosed, except as statistical totals or as otherwise authorized for the protection of the respondent rather than for purposes of national security.

Definition: 'confidentiality'

The Census Bureau's commitment to confidentiality guarantees that all information collected under the authority of Title 13 that would identify a respondent will be held, by law, in strict confidence.

Maintaining confidentiality

Here are a few guidelines to help you maintain a respondents' confidential information:

- Never reveal any personal information (for example, name or address) about a respondent, either orally or by allowing someone to read the questionnaire.
- Notify your supervisor immediately if materials containing census-confidential information are missing, stolen, or destroyed.
- When conducting interviews on the telephone, do not allow unauthorized persons to listen to the conversation.
- You may use a cordless or wireless phone when interviewing only with a respondent's permission before proceeding, since there is a possibility that the conversation could be picked up by radio or television receivers.
- Do not permit persons other than sworn Census employees to listen to an interview between you and a respondent. If friends or family members who are not included in the survey are present, ask respondents if they wish to be interviewed privately.
- Place census questionnaires and other materials in a locked drawer or brief case in your home if possible; otherwise, keep them in a place that prevents unauthorized persons from looking at the collected data.
- Do not leave census materials in view when in your vehicle. Keep your vehicle locked when unattended.
- Give old or used materials containing census-confidential information to your supervisor to forward to the office for destruction.
- Do not allow family or friends to accompany you or your staff when performing census activities in the field unless they are sworn Census employees.
- Do not allow non-Census sworn employees (for example, friends or family members) to deliver completed questionnaires to the scheduled drop site.
- Do not give out any addresses that you collect.

Penalty for breaching confidentiality

Whoever publishes or communicates any information, the disclosure of which is prohibited under the provisions of Section 9 of Title 13, and which comes into their possession by reason of being employed by the Census Bureau, shall be fined not more than \$250,000, or imprisoned not more than five years, or both.

Data Stewardship

The U. S. Census Bureau workforce is bound by an ironclad commitment that is backed by federal law: We may not release personally identifiable information (PII). **Data Stewardship** – providing quality data for public good while respecting individual privacy and protecting confidentiality – is the Census Bureau’s core responsibility. It is the formal process we use to care for the public’s information – from the beginning, when they answer a survey, to the end, when we release statistical data products.

The practice of data stewardship assures that the Census Bureau can effectively collect (and customers can use) high quality data while fully meeting the legal and reporting obligations levied by the Census Act (Title 13), the Privacy Act, and other applicable statutes, including the requirements of governmental and other suppliers of data to the Census Bureau. It also includes meeting higher ethical standards as identified by our privacy principles and other data stewardship best procedures and practices.

Keeping the public’s trust is critical to our ability to carry out our mission as the leading source of quality data about the nation’s people and economy.

Fax

Transmit PII only to secure fax machines. The sender should notify the recipient to expect a secure document and the receiver should notify the sender that the transmission has been received and secured. An unsecured fax of PII information is not authorized and is considered breach.

Mailing and Shipping

- All PII that is shipped using an overnight carrier that using tracking number, must be accounted for by the responsible party.
- The package contents must be double wrapped. On the inner wrapping put a confidentiality label that reads: “Disclosure Prohibited. Contents are confidential/restricted and protected by Title 13 and or may contain PII. To be opened by addressee only. On the outer package affix another confidentiality label. The label should contain the following information “Disclosure Prohibited”. Contents are confidential and covered by Title 13 and/or Title 15. To be opened by addressee only”

- Print and affix the shipping label. Do not use air bill for shipping. These are not authorized and do not allow for efficient tracking.
- Enclose a list of contents being transmitted.
- Seal and reinforce all packages being transmitted. The outer packaging should be clearly wrapped with yellow tape for easy identification that it contains PII.
- Notify the addressee of the shipment and its content.
- The sender should then make sure the package is dropped off or picked up by an authorized representative and track the package to make sure it is delivered to the recipient in a timely fashion. At no time should any materials be left with an external source for pick-up (e.g. with the hotel front desk, or host organization at a training site).
- A person designated in the ACO is responsible for monitoring the log to make sure that all PII shipments are entered and tracked to make sure they are delivered on time. If the ACO employee is shipping from the field, the field employee should send an email message to a designated mailbox with the tracking information, point of departure, and a description of the materials. A designated ACO employee should enter that information into the log.
- Use only shipping contractors who provide tracking services. (For overnight delivery, use the authorized package shipping service.)
- Ensure carriers understand that multiple packages containing “Census Confidential” material must travel and
- Be delivered as a unit.

**Transmitting
Assessment Materials**

*(Used in rare
circumstances)*

Special guidance is provided on the shipment of assessment materials due to the large amount of PII contained in applications and resumes. It is critical that Recruiting Assistants in the field coordinate the shipment and receiving of assessment materials with the Recruiter and/or administrative staff in the ACO. Outlined below is the process to be used for the 2020 Census.

1. After the completion of the assessment, the assessment administrator must immediately email the information from the D-969, Test Sign-In Sheet to the ACO Recruiting Department. The information on the D-969, includes:
 - a. Date of assessment session
 - b. Time of assessment session

- c. ACO number
- d. ACO mailing address
- e. Assessment site name
- f. Assessment site contact name and phone number
- g. Assessment site address, and
- h. Name, phone number, and county of each applicant

Sending the message allows the ACO to have a list of the applicant's names that took the assessment, which can be provided to the Incident Security Team if there is a data breach.

2. Applicant testing materials must be inventoried to account for all forms and documents for each applicant, along with a status of all applicant materials. If the applicant left the assessment session early and took their application materials with them, this should be noted on the D-969 and in the message sent after the session
3. The applicant folders from the testing session must be securely double wrapped with a confidentiality label on the bundle. Make sure you include the original D-969 and the D-315, *Testing Summary and Transmittal*. Any non-testing session materials should NOT be included with the test materials and do not bundle with another testing session.
4. Package the materials in an approved shipping box or envelope and send a second message to the ACO Recruiting Department, the second message should include:
 - a. The shipment tracking number,
 - b. The date, time, and location of the assessment session, and
 - c. The date and departure location of the shipment.

Including the above information in the second message will allow the Recruiting Department to match the shipping information to the information from the D-969.

All assessment materials should be sent "Standard Overnight" by no later than close of business on the day after the assessment was scheduled. Assessments

that take place on Fridays must be shipped no later than first thing Monday morning. The package must be either dropped off at the approved shipping facility or placed in a secure shipping mailbox.

5. ACO office staff should enter the information in the email into the PII log. The appropriate ACO staff should monitor the return of assessment materials against the PII log and report any delays to the appropriate supervisor immediately.
6. Upon receipt, assessment materials should be delivered to the appropriate person in the ACO. The recruiting database should have a tool in place that accounts for the receipt of assessment materials for every test session. With the large number of assessment sessions that can be scheduled at one time, it is recommended that the recruiting database be modified, if necessary, to have a “check-in” feature for confirming that assessment materials have been received by the recruiter or administrative staff.
7. Seal and reinforce all packages being transmitted.

Never use your personal e-mail account, such as, your AOL, Yahoo, Hotmail, or any other personal e-mail account to send Title 13 data, which includes information about the addresses you are working with or the information collected from a census respondent.

Never use your personal e-mail account to send Personally Identifiable Information (PII), such as the name and address, name and Social Security number, or other information that could be used to identify another person.

Also, never send e-mail with attachments to your Area Census Office (ACO). These attachments may contain hidden computer viruses that damage census files or create a security risk.

Finally, be aware that if you use your personal e-mail account for work related business, the messages could be used as evidence in an investigation (for example, if a complaint is filed by another employee). The Census Bureau does not require you to use your personal e-mail to do your job and will **NOT** provide reimbursement for your Internet connection or the use of your personal e-mail account.

Please refer questions about the definition of Title 13 or PII to your supervisor.

About the use of personal e-mail account(s)

Topic 4: False Statements and Information

Help to maintain the quality of collected census data

You are expected to help maintain the quality of census data by following written procedures, asking questions as worded on the questionnaire, and accurately recording responses that are communicated to you.

Penalties for falsifying data and information

If you willfully falsify information collected under Title 13, United States Code, Section 213, you can be found guilty of perjury (fabrication) and may be fined up to \$250,000 and/or imprisoned up to five years.

If it is determined that falsification was intentional, you will be removed from federal service.

Subpoenas

If you receive a subpoena for any census information, or other matters relating to your job, notify your supervisor and the Area Census Office Manager (ACOM) immediately.

Topic 5: Political Activity

Restrictions on your political activities

Under the 1939 Hatch Act, federal employees, among others, faced significant restrictions on their ability to participate in political activities. Congress amended the Hatch Act in 1993 to permit more political activity by federal employees. With the 1993 amendments, many federal employees are now permitted to take an active part in political management or in political campaigns. The Department of Commerce (DOC), of which the Census Bureau is a part, is covered by the 1993 amendments. Therefore, temporary, part-time, and regularly scheduled Census Bureau employees are covered by provision of the Act and may participate more freely in political activities.

The following '*Do's and Don'ts*' provide a brief summary for your review.

Federal Hatch Act Do's

Census Bureau employees covered by the 1993 amendments may:

- be candidates for public office in nonpartisan (that is, not affiliated with an individual political party) elections. However, if elected, an employee must resign their Census Bureau appointment or decline the elected position.
- register and vote as they choose
- assist in voter registration drives
- express opinions about candidates and issues
- contribute money to political organizations
- attend political fund-raising functions
- attend and be active at political rallies and meetings
- join and be an active member of a political party or club
- sign nominating petitions
- campaign for or against referendum questions, constitutional amendments, municipal ordinances
- campaign for or against candidates in partisan elections
- make campaign speeches for candidates in partisan elections
- distribute campaign literature in partisan elections
- hold office in political clubs or parties

**Federal Hatch Act
Don'ts**

Census employees covered by 1993 amendments **may not**—

- use official authority or influence to interfere with an election
- solicit or discourage political activity of anyone with business before the agency
- solicit or receive political contributions
- be candidates for public office in partisan elections
- engage in political activity while—
 - on duty
 - in a government office
 - wearing an official uniform
 - using a government vehicle
- wear political buttons on duty
- solicit or accept volunteer services from a subordinate for any political purpose

**Federal Hatch Act
Summary**

The '*Do's and Don'ts*' listed above are intended to provide an overview of permissible activities and restrictions; the listing is not intended to include all policies relating to employee participation in political activities. While the primary responsibility in the federal government for provision of advisory opinion and enforcement functions relating to the Hatch Act rests with the U.S. Office of Special Counsel (OSC), your first contact for questions should be with the Census Bureau's Employee Relations Branch, 301-763-3701.

More information about the Hatch Act and political activity rules can be found at the DOC Ethics Law and Programs Division's web site, www.commerce.gov/ethics.

Please remember that it is your responsibility to raise any questions or concerns about permissible political activities to your supervisor, local management, and appropriate offices within the Bureau. Otherwise, if after having received and investigated a complaint of a Hatch Act violation OSC finds violations warranting prosecution, an employee may be removed from a federal position or suspended from duty without pay. Federal employees should be aware that certain political activities may also constitute criminal offenses under Title 18 of the U.S. Code.

Topic 6: Outside Activities and Conflicts of Interest

Restrictions on your outside activities

You are prohibited from holding outside employment or conducting outside activities that are incompatible with fulfilling your census duties and responsibilities.

- Outside activities must not involve, or appear to involve, a conflict of interest.
- Outside activities must not interfere with or be detrimental to the efficient completion of your duties during the hours you are expected to be available for work.
- Outside employment must not interfere with the completion of your census assignment. Consult with your supervisor on any outside employment or other outside activity matter to ensure it does not raise a question of a conflict of interest.

Conditions that might affect public trust or your job performance

Below are a few conditions or situations that may create confusion in the respondent's mind as to whom you represent and affect the public's trust in the Bureau of the Census or possibly your ability to do your job. (*Other conditions may apply.*)

- Your employment as a law enforcer, tax collector, social worker, or door-to-door salesperson, and so forth, and as a Census Bureau employee might confuse a respondent as to whom you will submit collected census data.
- Outside activities that may cause you to be unavailable for census duties or perhaps reduce the time required to successfully perform your census duties.
- Your use of names or addresses of respondents from lists gathered by the Census Bureau to contact persons solely for the benefit of your outside activities. The use of federal government resources for the purpose of fulfilling duties associated with outside activities is prohibited.

Prohibited activities

You may not accept a fee, compensation, gift, payment of expense, or any thing of monetary value in cases which acceptance may result in, or create the appearance of, a conflict of interest.

You may not participate in any outside activity that might result in, or create the appearance of:

- using your public office for personal gain,
- giving preferential treatment to any person or organization,
- interfering with government efficiency or economy, or
- adversely affecting the public trust.

Dual federal employment

A person cannot hold two federal positions simultaneously if one is a full-time position, unless there is an agreement in place with that agency. If you are currently employed either full-time or part-time or are soon to be employed at another Federal agency while working at the Census Bureau, this might be regarded as dual federal employment. You must inform your supervisor at the Census Bureau if you are currently employed, or become employed, at another Federal agency.

Informing your office of possible dual federal employment

You must inform your supervisor (or the administrative staff at your Area Census Office) of any other federal agency or postal service where you might be currently working or will soon be working.

Submit a letter to your supervisor that includes--

- Your name, home address, phone number
- Name of federal agency, your position title, and a brief description of job duties and responsibilities.

The letter will be forwarded to the Regional Census Center Administrative Coordinator for review. If it is found that dual federal employment has, or will occur, your appointment may be ended.

Exemption from the dual Federal employment rule

If you work for the United States Postal Service (USPS), or an agency the Census Bureau has an agreement with, you may be exempt from the dual federal employment limitation; however, your Regional Census Center must still approve of this employment. Prepare a letter detailing your USPS employment including your name and home telephone number, and submit it to your supervisor who will forward it to the administrative staff for review and approval.

Topic 7: Post-Employment Restrictions Under 18 U.S.C. 207

Post-employment restrictions

The law (18 U.S.C. 207) places certain restrictions on the post-employment activities of former federal employees. The penalties for violating the provisions of the law are criminal in nature. Please refer to Illustration 1, Post Employment Restrictions on page 2-17.

The post-employment restrictions are summarized as follows:

General Restrictions:

1. A permanent bar on serving as a representative for another person or organization before any Federal agency or in a Federal court with respect to a particular matter involving specific parties in which you participated personally and substantially as a Government employee.
2. A two-year bar on serving as a representative for another person or organization before any Federal agency or in a Federal court with respect to a particular matter involving specific parties that was under your official responsibility during your last 12 months of Government employment.
3. A prohibition on using any no-public information acquired from your Government position for any personal purpose as long as the information remains confidential or protected from release to the public.

Special Restrictions:

1. Bar on accepting payments for lobbying/representational activities of others which occurred during the period of your government employment.
2. Limitations on misusing or disclosing nonpublic (for example, Privacy Act) information.
3. Limitations on testifying in court on United States matters.

There are four other general restrictions and five other special restrictions that apply only to senior employees or other exclusive personnel.

These statutory restrictions are fully explained in 18 United States Code, Section 207. If you have any questions, you may write the Assistant General Counsel for Administration, Department of Commerce, or call (202) 482-5387.

Topic 8: Summary of Ethics Rules

Summary of ethics rules

As an employee of the U.S. Department of Commerce, Census Bureau, you are subject to ethics rules and principles that apply to all federal employees. Please refer to Illustration 2, Top 10 Ethic Rules for 2020 Census Employees on page 2-18 and Illustration 3, General Ethics Principles on page 2-19 and Illustration 4, Summary of Ethics Rules on page 2-20 for additional guidance.

Maintaining confidentiality of information

You may not disclose or use any information that you have obtained as a Census employee and that has not been released to the public, including any data that you have collected while doing your government job.

Misuse of government position

You may not use government time, equipment, or your government title for your personal activities. ‘Equipment’ includes government personal and mobile devices, laptops, tablets, fax machines, photocopiers, stationery, vehicles, and staff.

You may not use your position as a census employee to benefit your friends, relatives, or people with whom you conduct business.

You may not ask an employee of the Department of Commerce to take action on a matter, such as a trade issue or a patent application, for anyone other than yourself. This includes writing a letter, making a telephone call, or meeting in person with a Department of Commerce employee. However, you may contact the Department to obtain information that is made available to the public.

Financial interests

Generally, you may not work on an assignment for the Bureau if it involves a company in which you have a financial interest. Your financial interests also include those of your spouse, minor child/children, general partner, private employer, an organization for which you serve as an officer or director, or a prospective employer.

Gifts

Generally, you may not accept a gift given to you because you are a Government employee. This includes a gift from someone who has any financial interest in the work you are doing, such as a city or county that has an interest in the census count or a company that contracts with your office. There are some exceptions: you may accept gifts of \$20 or less or gifts from relatives and friends.

You may not give a gift to your supervisor or accept a gift from anyone you supervise unless it is for a special occasion (such as, marriage or retirement) or for holidays or birthdays and the gift costs \$10 or less.

Office of the General Counsel

For further advice regarding any of these matters, call the Ethics Division, Office of the Assistant General Counsel for Administration, and ask for an advisor at (202) 482-5384.

If you would like a written ethics opinion, write to:

Assistant General Counsel for Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Room 5876
Washington, D.C. 20230

Standards of conduct text

The complete text of the government-wide standards of conduct for federal employees is available on the internet. The internet address is www.usoge.gov.

Illustration 1 Post Employment Restrictions

D-287 (5-31-2018)



U.S. DEPARTMENT OF COM
Economics and Statistics Admini
U.S. CENSUS t

POST EMPLOYMENT RESTRICTIONS UNDER 18 U.S.C. 207 2020 Census

The law (18 U.S.C. 207) places certain restrictions on the post employment activities of former federal employees. The penalties for violating the provisions of the law are criminal in nature.

The post employment restrictions are summarized as follows:

General Restrictions:

- 1.** A permanent bar on serving as a representative for another person or organization before any Federal agency or in a Federal court with respect to a particular matter involving specific parties in which you participated personally and substantially as a Government employee.
- 2.** A two-year bar on serving as a representative for another person or organization before any Federal agency or in a Federal court with respect to a particular matter involving specific parties that was under your official responsibility during your last 12 months of Government employment.
- 3.** A prohibition on using any non-public information acquired from your Government position for any personal purpose as long as the information remains confidential or protected from release to the public.

Special Restrictions:

Additional post employment restrictions apply to former senior employees (employees whose basic pay was greater than \$155,440) and former political appointees.

If you have any questions about the post-employment restrictions contact the DOC Ethics Law and Programs Division at 202-482-5384 or ethicsdivision@doc.gov. Further information about the post-employment restrictions is available on the Ethics Law and Programs Division's web site, www.commerce.gov/ethics.

Illustration 2

Top 10 Ethics Rules For 2020 Census Employees

FORM D-472 (6-11-2018)



U.S. DEPARTMENT OF COMMERCE
Economics and Statistics Administration
U.S. CENSUS BUREAU

TOP 10 ETHICS RULES FOR EMPLOYEES 2020 Census

USE OF GOVERNMENT RESOURCES – AVOID MISUSE OF RESOURCES

1. **Do not** use your Government resources or staff for personal activities, including political activities.
2. **Do not** take any action that will create an appearance of misuse of your Government position for personal benefit.

GIFTS – AVOID UNDUE INFLUENCES

3. **Do not** accept a gift from anyone that has an interest in U.S. Department of Commerce activities unless an exception applies. (Common exceptions are: (1) \$20 or less in value,* (2) an invitation to a "widely attended gathering" and your supervisor has approved,* (3) from a friend or relative, or (4) from a foreign government,*) ** note that this exception does not apply to gifts or invitations to a political appointee from a lobbying organization (unless it is a media company or a 501(c) (3) organization)*
4. **Do not** give a gift to a supervisor or accept a gift from a subordinate unless it is: (1) for a major life event, (2) \$10 or less in value, or (3) a host/guest gift.

PERSONAL RELATIONSHIPS – AVOID APPEARANCES OF FAVORITISM

5. **Do not** participate in any matter in which one of the parties is someone with whom you have a close personal or business relationship.

OUTSIDE ACTIVITIES – AVOID DIVIDED LOYALTIES

6. **Do not** engage in outside employment or outside activities with non-Federal entities that have matters before your office.
7. **Do not** contact a Federal official on behalf of someone else to influence Government action, unless it is part of your Government duties.

POLITICAL ACTIVITIES – KEEP POLITICS AND GOVERNMENT SEPARATE

8. **Do not** engage in political activities while on Government premises or during duty hours and do not engage in political fund-raising at any time.

FINANCIAL CONFLICTS OF INTEREST – AVOIDED SELF-DEALING

9. **Do not** participate in a matter that will affect your financial interests (such as a company in which you own stock), unless the interest is minimal.

SEEKING EMPLOYMENT AND POST-EMPLOYMENT RESTRICTIONS

10. **Do not**, during the period of a job search, participate in a matter in which a prospective employer has a financial interest.

*Prepared by the Ethics Law and Programs Division, Office of the Assistant General Counsel for Administration, United States Department of Commerce 202-482-5384
ethicsdivision@doc.gov – May 25, 2018*

Illustration 3

General Ethics Principles

D-473 (5-31-2018)



GENERAL ETHICS PRINCIPLES

2020 Census

U.S. DEPARTMENT OF COMMERCE
Economics and Statistics Administration
U.S. CENSUS BUREAU

1. Public service is a public trust, requiring employees to place loyalty to the Constitution, the laws and ethical principles above private gain.
2. Employees shall not hold financial interests that conflict with the conscientious performance of duty.
3. Employees shall not engage in financial transactions using nonpublic Government information or allow the improper use of such information to further any private interest.
4. An employee shall not, except as permitted in ethics regulations, solicit or accept any gift or other item of monetary value from any person or entity seeking official action from, doing business with, or conducting activities regulated by the employee's agency, or whose interests may be substantially affected by the performance or non-performance of the employee's duties.
5. Employees shall put forth honest effort in the performance of their duties.
6. Employees shall not knowingly make unauthorized commitments or promises of any kind purporting to bind the Government.
7. Employees shall not use public office for private gain.
8. Employees shall act impartially and not give preferential treatment to any private organization or individual.
9. Do not engage in political activities while on Government premises or during duty hours.
10. Employees shall not engage in outside employment or activities, including seeking or negotiating for employment, that conflict with official Government duties and responsibilities.
11. Employees shall disclose waste, fraud, abuse, and corruption to appropriate authorities.
12. Employees shall satisfy in good faith their obligations as citizens, including all just financial obligations, especially those—such as Federal, State, or local taxes—that are imposed by law.
13. Employees shall adhere to all laws and regulations that provide equal opportunity for all Americans regardless of race, color, religion, sex, national origin, age, or handicap.
14. Employees shall endeavor to avoid any actions creating the appearance that they are violating the law or the ethical standards set forth in ethics regulations. Whether particular situations create an appearance that the law or these standards have been violated shall be determined from the perspective of a reasonable person with knowledge of the relevant facts.

Prepared by the Ethics Law and Programs Division, Office of the Assistant
General Counsel for Administration, United States Department of Commerce
202-482-5384
ethicsdivision@doc.gov
May 25, 2018

Illustration 4

Summary of Ethics Rules

D-187
(5-31-2018)

U.S. DEPARTMENT OF COMMERCE
Economics and Statistics Administration
U.S. CENSUS BUREAU



2020 Census

As an employee of the U.S. Department of Commerce, Census Bureau, you are subject to ethics rules and regulations, that apply to all federal employees. Please carefully read the following summary of the more important rules.

Misuse of Government Position

- You may not use government time, equipment, or your government title for your personal activities. Equipment includes government computers, fax machines, photocopiers, stationery, vehicles, and staff.
- You may not use your position as a Census Bureau employee to benefit your friends, relatives, or people with whom you conduct business.
- You may not ask an employee of the Department of Commerce, or any other federal agency or court, to take action on a matter, such as a trade issue or a patent application, for anyone other than yourself. This includes writing a letter, making a telephone call, or meeting in person with a Commerce Department employee. However, you may contact the Commerce Department to obtain information that is made available to the public.

Outside Activities and Employment Restrictions

- You may be involved in activities or employment outside the federal government as long as they are not similar to your government job, and do not prevent you from doing your government job.

Financial Interests

- Generally, you may not work on an assignment for the Census Bureau if it involves a company in which you have a financial interest. Your financial interests also include those of your spouse, minor child, general partner, private employer, an organization for which you serve as an officer or director, or a prospective employer.

Gifts

- Generally, you may not accept a gift given to you because you are a government employee. This includes a gift from someone who has any financial interest in the work you are doing, such as a city or county that has an interest in the census count or a company that contracts with your office. There are some exceptions: you may accept gifts of \$20 or less or gifts from relatives and friends.
- You may not give a gift to your supervisor or accept a gift from anyone you supervise unless it is for a special occasion (such as marriage or retirement), or it is for holidays or birthdays and the gift costs \$10 or less.

Office of the General Counsel

For further advice regarding any of these matters, call or email the Ethics Law and Programs Division at 202-482-5384 or ethicsdivision@doc.gov. If you would like a written ethics opinion, write to:

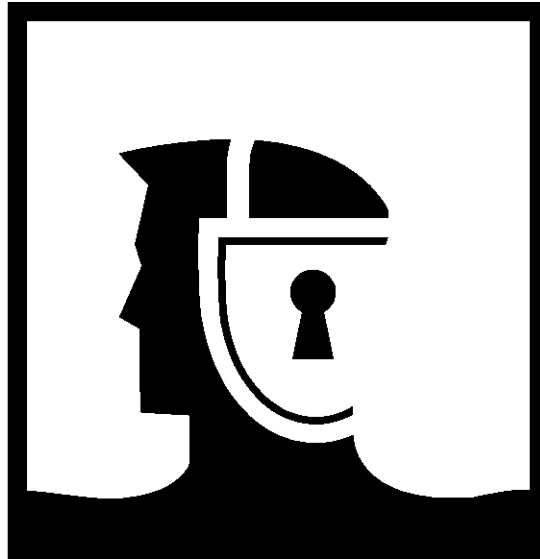
Ms. Barbara S. Fredericks
Assistant General Counsel for Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 5875
Washington, DC 20230

Standards of Conduct Text

A complete text "Summary of Ethics Rules for New Employees" is available at www.commerce.gov/ethics

D-187 (5-31-2018)

CONFIDENTIALITY



Shh...keep all census data confidential!

Never reveal any information about a respondent, either verbally or by allowing someone to read the questionnaires.

Place confidential materials in a locked area when not in use.

Chapter 3: Personnel and Payroll

Topic 1: Your Appointment

Appointment document

Your appointment document is a Standard Form (SF) 50, *Notification of Personnel Action*. A SF-50 is produced for most personnel actions that you will experience. The SF-50 provides a chronological record of employment and personnel actions processed. It shows the appointment effective date, hourly rate of pay, your name, and other personnel data about your job. Keep this document and any other SF-50s you receive through the duration of your employment in a safe place. It can be used to verify your federal service with the Census Bureau when seeking other federal employment.

Position title/work schedule

Your position title is shown in Item #15 and your work schedule is shown in Item #32 on your SF-50.

Length of appointment

You are appointed to a temporary Schedule A appointment with a specific Not-to-Exceed (NTE) date or expiration date. You may be released from service with the Census Bureau before this appointment's NTE date if work or funds are no longer available. The expiration date of your appointment does not guarantee the availability of work or your services. Depending on the availability of the work, your appointment may be extended.

Upon completion of your service, you will receive a 1) SF-50, *Notification of Personnel Action* documenting the date you separated from the Census Bureau and a 2) SF-8, *Notification to Federal Employee about Unemployment Insurance* documenting the 3-digit Identification Federal Agency (914) that you worked for. Take these forms with you when you file your unemployment claim to indicate that you were employed and to help expedite your claim.

Please note that the 914 code should **only** be used by employees who performed work for the 2020 Census. It should **never** be used by employees who performed work on current surveys or other non-decennial related work.

Benefits

To further the goal of providing affordable health insurance to Federal employees the Office of Personnel Management (OPM) published a final rule (79 FR 62325) on October 17, 2014, modifying and expanding Federal Employees Health Benefits Program (FEHB) enrollment eligibility to certain employees on intermittent work schedule. Employees under an intermittent work schedule, who are expected to work in their appointment for at least 90 days and are expected to work 130 or more hours in a calendar month are eligible to enroll in FEHB. Eligible employees who enroll in FEHB will receive the same government contribution towards the FEHB premium costs as full-time permanent employees.

When employees are eligible, they will receive an FEHB Eligibility Notification Letter, via e-mail. Please note that Recruiting Assistants, Clerks and Office Operations Supervisors will be eligible on their hire date. However, Enumerators and Census Field Supervisors will not be eligible until they reach 90 days and 130 hours in a calendar month. If an employee plans to enroll or waive FEHB coverage, they must complete and return an SF-2809, Health Benefits Election Form within 60 days from the date of the email.

FEHB coverage will become effective on the first day of their pay period after their personnel office receives and processes their complete SF-2809.

Each pay period they are enrolled in the FEHB Program they are responsible for payment of the employee share of the premium. When their earnings for the week are insufficient to cover the premium or they submit a late timesheet, they will incur an FEHB debt. They will receive a debt notification letter. This letter will include the details of their debt, repayment options and response deadlines. They must be sure to respond to this letter within 30 days from the date of the notice and return the Decision Letter, or their FEHB coverage will be terminated.

They are also eligible to participate in the Healthcare Flexible Spending Account (HCFSA) and Federal Long Term Care Insurance Program (FLTCIP). Eligibility in these programs are based on their eligibility for FEHB; however, they do not have to

enroll in FEHB to participate in HCFSA and/or LTC, and vice versa. As a result, they must set up a payment method with HCFSA and/or FLTCIP, when they complete their enrollment on their website.

Employees assigned to an intermittent work schedule are paid only for the hours worked, and the number of hours can vary depending on the nature of the work assignment. Intermittent employees:

- Do not earn or use paid annual (personal) or sick leave.
- Are not eligible for life insurance coverage.
- Are not eligible for federal retirement coverage.
- Are not eligible to participate in the Thrift Savings Plan.

Retirement coverage

Your earnings are taxed for and covered by the Medicare Tax Program and the Federal Insurance Contributions Act (*Social Security*). For each of these taxes, your D-444, *Earnings Statement*, will identify a specific amount withheld from your gross salary.

Post of duty

Your post of duty (*official workstation*) is the state and county of your home. Your workday can begin and end at your home. (*As a reminder, keep census information confidential from all persons not employed by the Census Bureau.*)

Hours of duty

You must be available as the work occurs. You are expected to work the most productive hours of the day. If you are interviewing, select a time when most residents are home and are able to respond. Experience has shown that the most productive times are usually evenings and weekends. If you work in excess of 5 consecutive hours in any day, you must take an unpaid meal period of 30 minutes.

Updating or correcting your employee information

It is your responsibility to notify the administrative section of the Area Census Office (ACO) when any part of your information changes or is incorrect. Complete Form D-149, *Correction Request Form*, and give it to your supervisor.

Chain of Command

Use the Chain of Command chart to determine the first and second level supervisors for field positions. Then refer to the Authority for Recommendation and Approvals chart on the next page to determine the type of actions they have authority to initiate/approve.

Table 3-1: Chain of Command

	FIRST LEVEL	SECOND LEVEL	THIRD LEVEL	FOURTH LEVEL
Enumerator	Census Field Supervisor (CFS)	Census Field Manager (CFM)	Lead Census Field Manager (LCFM)	Area Census Office Manager (ACOM)
Census Field Supervisor (CFS)	Census Field Manager (CFM)	Lead Census Field Manager (LCFM)	Area Census Office Manager (ACOM)	Area Manager
Recruiting Assistant (RA)	Recruitment Manager	Area Census Office Manager (ACOM)	Area Manager	
Clerk	Office Operations Supervisor (OOS)	Census Field Manager, Administrative Manager, Recruitment Manager, IT Manager	Area Census Office Manager (ACOM)	Area Manager
Office Operations Supervisor (OOS)	Census Field Manager, Administrative Manager, Recruitment Manager, IT Manager	Area Census Office Manager (ACOM)	Area Manager	Assistant Regional Census Manager (ARCM)
Administrative Manager	Area Census Office Manager (ACOM)	Area Manager	Assistant Regional Census Manager (ARCM)	Deputy Regional Director (DRD)
Census Field Manager	Lead Census Field Manager (LCFM)	Area Census Office Manager (ACOM)	Area Manager	Assistant Regional Census Manager (ARCM)
Lead Census Field Manager	Area Census Office Manager (ACOM)	Area Manager	Assistant Regional Census Manager (ARCM)	Deputy Regional Director (DRD)
IT Manager	Area Census Office Manager (ACOM)	Area Manager	Assistant Regional Census Manager (ARCM)	Deputy Regional Director (DRD)
Recruitment Manager	Area Census Office Manager (ACOM)	Area Manager	Assistant Regional Census Manager (ARCM)	Deputy Regional Director (DRD)
Area Census Office Manager (ACOM)	Area Manager	Assistant Regional Census Manager (ARCM)	Deputy Regional Director (DRD)	

Table 3-2: Authority for Recommendation and Approvals

	ENUMER	CFS	CLERK	OOS	ADMIN MGR	CFM	IT MGR	REC MGR	LEAD CFM	ACOM	AREA MANAGER
Recommends overtime for approval for one level lower... completes the CD-81		✓		✓	✓	✓	✓	✓	✓	✓	✓
Approves overtime... signs the CD-81					✓	✓	✓	✓	✓	✓	✓
Counseling Documentation regarding Conduct or Performance... Recommends termination for one level lower... completes the D-282		✓		✓	✓	✓	✓	✓	✓	✓	✓
Approves termination for two levels lower... approves and completes the D-283					✓	✓	✓	✓	✓	✓	✓
Recommends employment changes including position conversions, promotions and retention for one level lower... completes D-291		✓		✓	✓	✓	✓	✓	✓	✓	✓
Approves staffing changes including two levels lower... approves the D-291		✓		✓	✓	✓	✓	✓	✓	✓	✓
Signs that the D-291, CD-81, D-282 and D-283 have been reviewed		✓		✓	✓	✓	✓	✓	✓	✓	✓

Topic 2: Your Salary

Hours

You will be paid at the trainee pay rate while in training. Training hours include classroom training, related on-the-job training (OJT) field work you receive from your supervisor, and if applicable, completing self-study assignments at home. Upon completion of the training, if you are converted to the full potential of your position (e.g., enumerator trainee to enumerator) you will be paid at the regular hourly rate of pay for working production hours. Production hours include time spent conducting interviews, canvassing neighborhoods, working on assignments in your home, and other related operational duties or activities not associated with training.

(See more on this in Topic 3, Your Job Activities and Authorized Hours, in this chapter.)

Pay periods

Pay periods are weekly beginning Sunday and ending Saturday.

Pay day

You will receive your first paycheck approximately 11 days after you complete your first week of work. Thereafter, you will be paid each Wednesday for every week or portion of a week you work.

Payroll processing schedule

The payroll section in your office will process all payroll documents received by noon each Wednesday. For example, if you submitted a D-308, *Daily Pay and Work Record* or E-308, *Electronic Daily Work Record*, for work performed during the weekly pay period beginning Sunday, March 4, 2018, and ending Saturday, March 10, 2018, then you will have access to your paycheck on Wednesday, March 21, 2018.

Note: Any payroll forms received after the processing cycle ends will be processed in the next payroll processing cycle. D-308 will only be used if employee cannot submit an electronic payroll form (E-308).

E-308, *Electronic Daily Pay and Work Record*

Field staff will use a device for submitting an electronic payroll form. Each day you worked, you will fill in the required entries including the date worked, type of hours and the start and end times and then transmit daily. You must process a separate E-308

transaction for each day that you worked, or if you have approved O/T for the day. For example, if you worked on field activities and preparation activities, you would complete an E-308 for the field worked and a second E-308 for the preparation time.

Form D-308, *Daily Pay and Work Record*

For operations that do not use a device or if the E-308 is not available or not working properly, your payroll document is a D-308. You must complete a separate D-308 for each day that you worked. Fill in the required entries including your name, the date and day, the number and type of hours, and the times of day that you worked. If you worked on more than one task or job activity in a single day, then you must complete a separate D-308 for each task. For example, if you worked on payroll and on recruiting activities, complete a D-308 for payroll and a second D-308 for recruiting activities.

Submission of your paper payroll form

Submit a completed D-308 to your supervisor for each day you worked. Your supervisor will review, certify, and forward your payroll document to the administrative section of your ACO for processing.

Direct deposit of paychecks

By establishing an Electronic Funds Transfer (EFT) or direct deposit, your paycheck is deposited into your checking or savings account at your financial institution (e.g., bank, credit union, etc.). You need not worry that your check was lost in the mail. If you are interested in direct deposit and did not complete a D-1199, *Payment Authorization*, online or at the training session, use the copy located in Appendix A at the back of this Handbook. Complete Section 1, 2 and 4. You may need to request a form from the office if your handbook is in a pdf form.

If you do not have a bank account and will not get one, you must complete section 3, request for waiver and section 4 of the D-1199, *Payment Authorization*. Incorrect data will cause a delay in receiving your paycheck. Submit the completed D-1199 to your manager or mail it directly to the ACO. You may need to request a form from the office if your handbook is in a pdf form.

Change in your routing or account number

It is your responsibility to notify the administrative section of the ACO when your financial institution notifies you that there is a change in the institution's routing number or your account number. A change to the routing number could be the result of a merger between two financial institutions. If the ACO is not notified timely, there may be a delay in receiving your paycheck.

Paper Checks

On April 26, 1996, the President signed into law legislation mandating the use of EFT for Federal Payments. Specifically, the Debt Collection Improvement Act of 1996 requires that, beginning July 26, 1996, all new employees receive their Federal wages and salaries via EFT. Effective January 2, 1999, all Federal payments, including Federal wages and salaries, paid to current employees are required to be made by EFT.

Rare circumstances in which a waiver may be granted are as follows:

- Do not have a bank account
- Hardship due to a physical or mental disability
- Financial hardship
- Geographic barrier
- Language barrier

If you want a paper check because you are unable to obtain an account from a financial institution, you are required to complete a D-1199. Paper checks are mailed to your home address or the mailing address, which you specified on your job application (BC-170).

Changing your address

To change your address at any time during your employment, complete D-149, *Correction Request* and give it to your supervisor. Your supervisor will submit the form to the ACO for update in DAPPS. All subsequent paychecks, earnings statements and human resource documents will be mailed to this address.

Checks that are lost or undeliverable due to an incorrect mailing address will be returned to the Department of the Treasury for automatic cancellation. A replacement check may take up to six weeks to be reissued. Using direct deposit avoids these situations.

Form D-444, Earnings Statements

For each week that you receive a paycheck you will receive an earnings statement in the mail. This earnings statement shows your total earnings and reimbursements for the weekly pay period as well as the year-to-date totals. These statements are printed in Jeffersonville, IN and may be received later than your paycheck.

An illustration of the D-444, *Earnings Statement*, is shown on page 3-10.

An error or non-receipt of paycheck and/or earnings statement

If you find an error or do not receive your paycheck and/or earnings statement, call your ACO administrative area or the Personnel and Payroll Hotline at 855-236-2020, option #3.

Illustration 3-1: D-444, Earnings Statement

New York Regional Office US Census Bureau 32 Old Slip, 9th Floor New York, NY 10005		Pay Group: CB1-Census Temporary Weekly Process On-Cycle Pay Begin Date: 08/13/2017 Check #: 000000000412643 Pay End Date: 08/19/2017 Check Date: 08/30/2017	
Testeight Interface 975 Smith St Providence, RI 02908	Employee ID: 30000228 Department: 2204-Providence County, RI Location: Rhode Isla - Kingston Job Title: Enumerator Pay Rate: \$18.000000 Hourly	TAX DATA: Federal RI State Tax Status: Single Single Allowances: 0 0 Addl. Pct.: Addl. Amt.:	

HOURS AND EARNINGS						TAXES		
Description	Rate	Current Hours	Earnings	YTD		Description	Current	YTD
				Hours	Earnings			
Mileage	0.535000	20.00	10.70	20.00	10.70	Fed Withholding	0.98	0.98
Other Reimbursement			20.00		20.00	Fed MED/EE	0.78	0.78
Regular	18.000000	3.00	54.00	3.00	54.00	Fed OASD/EE	3.35	3.35
						RI Withholding	2.03	2.03
Total:		23.00	84.70	23.00	84.70	Total:	7.14	7.14

BEFORE-TAX DEDUCTIONS			AFTER-TAX DEDUCTIONS		
Description	Current	YTD	Description	Current	YTD
Total:	0.00	0.00	Total:	0.00	0.00 * Taxable

TOTAL GROSS	FED TAXABLE GROSS	TOTAL TAXES	TOTAL DEDUCTIONS	NET PAY
Current: 84.70	54.00	7.14	0.00	77.56
YTD: 84.70	54.00	7.14	0.00	77.56

NET PAY DISTRIBUTION	
Check #000000000412643	77.56
Total:	77.56

Income tax deductions

Federal, state, and local (*where applicable*) income taxes will be deducted from your earnings each pay period. The amounts withheld will be based on the number of exemptions you requested on the *Withholding Allowance Certificate*, you completed on your first day of training.

If you wish to change your non-federal exemptions at any time during your employment, complete a separate Tax Withholding Statement for that state, city, or county. If you want to change your federal exemption status or claim 10 or more exemptions from withholding, you **must** complete a W-4. Give the completed document(s) to your supervisor to forward to the ACO for processing.

Note: Federal tax forms can be obtained from the internet at www.irs.gov.

Requests for overtime hours

The appropriate manager or designee must approve all requests for overtime hours in advance, before you begin working the additional hours. If you work overtime without supervisory approval, you will be subject to termination. Refer to Topic 3 for the complete overtime policy.

Non-compensable time

Non-compensable (*unofficial*) time includes lunch breaks, breaks to run personal errands, and any other time not spent conducting official census duties. If you are on official duty and take a break, do not record this time as paid time on your payroll document. Subtract this time from your total daily hours worked. You are paid only for the hours that you actually work.

Topic 3: Your Job Activities and Authorized Hours

Census Bureau overtime policy for Enumerators

Overtime is defined as hours of work ordered and approved in advance in writing by the appropriate manager or designee that exceeds 8 hours in a day or 40 hours in a week (Sunday through Saturday). You are not permitted to work more than 40 hours weekly. This work time includes preparing assignments, completing assignments in the field or office, and traveling to and from your assignment area. It is grounds for termination if you exceed this limit without advance approval.

You are not permitted to work more than 8 hours in a day. If overtime is necessary, the appropriate manager will approve the overtime hours before you begin working. If you work overtime without supervisory approval, you will be subject to termination.

In compliance with the applicable statutes and regulations, the Census Bureau has set rules and procedures for monitoring and compensating overtime hours worked.

You are not allowed to manipulate hours, for example, working 42 hours in one week, but reporting the excess hours during a subsequent week in which you have worked less than 40 hours. Manipulating hours is grounds for termination.

If you work more than 40 hours in a week without supervisory approval, you will be subject to termination unless the overtime was caused by “unavoidable circumstances.” “Unavoidable circumstances” are defined as unforeseeable circumstances beyond the employee’s control. They include, but are not limited to, weather-related problems such as a blizzard, flood, hurricane, etc. Traffic is not considered an “unavoidable circumstance” unless you are involved in an accident, delayed by an accident or unforeseen road conditions.

By signing the *Temporary Excepted Service Employment Agreement and Overtime Policy Agreement* at the time of your hiring you agreed to abide by these regulations.

Census Bureau overtime policy for Recruiting Assistants

Overtime is defined as hours of work ordered and approved in advance in writing by the appropriate manager or designee that exceeds 8 hours in a day or 40 hours in a week (Sunday through Saturday). You are not permitted to work more than 40 hours weekly. This work time includes preparing assignments, completing assignments in the field or office, and traveling to and

from your assignment area. It is grounds for termination if you exceed this limit without advance approval.

You are not allowed to manipulate hours, for example, working 42 hours in one week, but reporting the excess hours during a subsequent week in which you have worked less than 40 hours. Manipulating hours as well as working unauthorized overtime are grounds for termination.

If you work more than 40 hours in a week without supervisory approval, you will be subject to termination unless the overtime was caused by “unavoidable circumstances.” “Unavoidable circumstances” are defined as unforeseeable circumstances beyond the employee’s control. They include, but are not limited to, weather-related problems such as a blizzard, flood, hurricane, etc. Traffic is not considered an “unavoidable circumstance” unless you are involved in an accident, delayed by an accident or unforeseen road conditions.

By signing the *Temporary Excepted Service Employment Agreement and Overtime Policy Agreement* at the time of your hiring you agreed to abide by these regulations.

Job activities and authorized hours

The following chart is a list of the type of hours you may work and when they would be recorded on a D-308 or E-308.

Table 3-3: Job Activities and Authorized Hours

HOURS	JOB ACTIVITIES	TIME AUTHORIZED
Training	<ul style="list-style-type: none"> • Traveling to and from the training site • Classroom training • On-the-job field training 	Up to 8 hours daily - your supervisor can help you determine your daily hours
Regular	<ul style="list-style-type: none"> • Traveling to and from the office for work-related purposes • Traveling to and from the job assignment area • Completing the assignment • Meeting with your supervisor • Reviewing job assignments with your supervisor • Other related official activities 	Up to 8 hours daily or 40 hours in a week
Overtime	<ul style="list-style-type: none"> • Hours of work ordered and approved in advance by the appropriate manager or designee that exceeds 8 hours in a day or 40 hours in a week 	<p>Only when requested and approved in advance by the appropriate manager or designee. Do not work overtime unless you have received approval from your supervisor.</p> <p>See the beginning of Topic 3 for the complete overtime policy.</p>

Topic 4: Reimbursable Expenses

What are reimbursable expenses?

Reimbursable expenses are those expenses that you incur performing your duties while on official census business and are reimbursed to you by the Census Bureau. Normally, you are provided with writing supplies and paper to do your job. Purchasing any such supplies must be approved by your supervisor before you make the purchase. Keep a copy of any receipts for you records.

What expenses will the Census Bureau reimburse?

The Census Bureau will reimburse you for the following expenses:

- Mileage - all miles you travel in your privately-owned vehicle (*or borrowed vehicle*) from your home to the training site or your job assignment area and the return trip; all miles that you travel while driving within your job assignment area to conduct census activities
- Local bus, trolley car, ferry, or subway fares
- Road, bridge, and tunnel tolls (*toll receipts must be attached to your payroll document when using D-308 and a picture of receipts transmitted with E-308*)
- Parking fees if free parking is not available while on official business in the field (*receipts from parking attendants must be attached to your payroll document*); parking fees for metered spaces
- Taxi fare **ONLY** when specifically authorized in advance
- Supervisor-authorized purchases (*attach receipt or photo of receipt with your payroll document for items costing more than \$5*)
- Official census duty business related local and long-distance calls made from your home, cellular or public telephone. **If you were issued a government phone, you are expected to use the government issued phone to make Census related business calls. In this instance you should not use your own home, cell or a public phone (unless there is an issue with your government issued phone not working properly). Only employees who work on the site and were not issued a government phone should claim reimbursement for home, cell or public phone charges.**

- Reimbursement will occur where those calls results in charges, in excess of existing plans, or excess that was caused by Census related calls. You must attach a detailed phone statement indicating those calls made for Census purposes to receive reimbursement.
- Per Diem for meals and lodging expenses when overnight travel is authorized (*if you are authorized per diem, your office will provide you with detailed instructions*)
- Payments to interpreters/facilitators hired to translate interviews with households or assist in group quarters; the hourly rate of pay is equal to that of an enumerator position

Submission of receipts when completing payroll

For all expenses over five (5) dollars, take a photo of the receipt using your device. Follow the steps within your device to submit the photo of the receipt along with your E-308. If the device is not available attach a copy of the receipt to a D-308 and give the filled out D-308 to your manager.

Using an interpreter

- Contact your supervisor to find an employee who can speak the necessary language to assist you.

Are there any expenses that the Census Bureau will not reimburse?

The Census Bureau will not reimburse you for the following expenses:

- Parking permits or other fees for your official duty station (*home*)
- Fees for the use of rental cars and taxis which are not authorized for the operation in which you work
- Mileage driven while doing personal errands, breaks, and other unofficial time
- Personal phone calls made from home, cellular, or public telephones which are not census-related
- Cellular phone basic service charges
- Purchases that your supervisor did not authorize
- Any purchase or expenditure (*even if approved*) costing more than \$5 for which you do not attach a receipt (or photo of receipt) to your payroll document
- Towing charges

- Speeding and/or parking tickets
- Gasoline, oils, antifreeze, tires, vehicle accessories
- Vehicle insurance premiums

Topic 5 : How to Complete Your Paper Daily Payroll Form

When to use

In the event you cannot complete your daily work and expenses electronically, you must complete a D-308, *Daily Pay and Work Record*, and submit it to your supervisor for each day you worked. An illustration of the D-308 is shown on the next page. Use the instructions below to complete your daily payroll form.

Item	Part A – Employee Information
Name	Enter your First Name, Middle Initial and Last Name
Employee ID number	Enter your Employee ID number.
1. Date worked, Day worked, Reclaim	Enter the date and mark an (X) in the box for the corresponding day worked. Mark an (X) in the RECLAIM box if you are reclaiming hours or expenses for a day that has already been paid.
2. Task code, Operation name	Enter the task code and the corresponding operation name that identifies the work you are performing. If you work on 2 or more tasks in one day, prepare a D-308 for each task code.
3. Office code and name	Enter the four-digit office code and the office name.
4. Points of travel	Enter the place to which you drove each day. When driving within a city or county, enter the abbreviation I&A for “in and around.” For example, “I&A Fairfax County and return.” OR, if you work in more than one assignment area, then enter only the AA numbers.
Item	Part B – Pay Information
1. Hours worked	Enter your daily hours of work (whole or partial hours) using the decimal system. <i>Do not include lunch periods or personal breaks.</i> 15 minutes = .25 30 minutes = .50 45 minutes = .75 a full hour = 1.00 <i>Examples: 4 hours and 15 minutes is represented as 4.25</i> <i>8 hours and 00 minutes is represented as 8.00</i>
2. Times of day worked	Enter the actual times of day that you work. <i>Do not include lunch periods or personal breaks. The times of day worked are required on every form submitted for payment. The times recorded here will be matched against the hours recorded, so enter this information accurately to avoid disallowances of hours and delays in receiving a full paycheck.</i>
3. Have you claimed ALL hours worked?	Record any hours you worked but are not claiming for payment. Also include the date(s) the hours were worked and an explanation of why you are not claiming them for payment.
4. Reimbursements	Enter your daily expenses incurred while on official business.
Cases Completed	<i>Do not make entries in this item.</i>
Item	Part C - Certification
Employee's Certification	Enter your signature and date at the time you meet with your supervisor to obtain approval of your work time.
Supervisor's Certification	<i>Do not make entries in this item.</i>

Illustration D-308, Daily Pay and Work Record

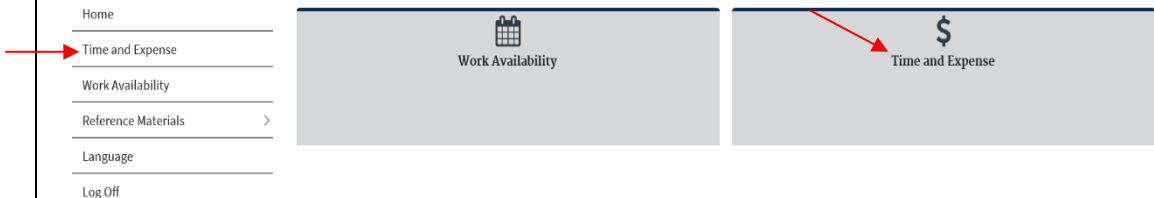
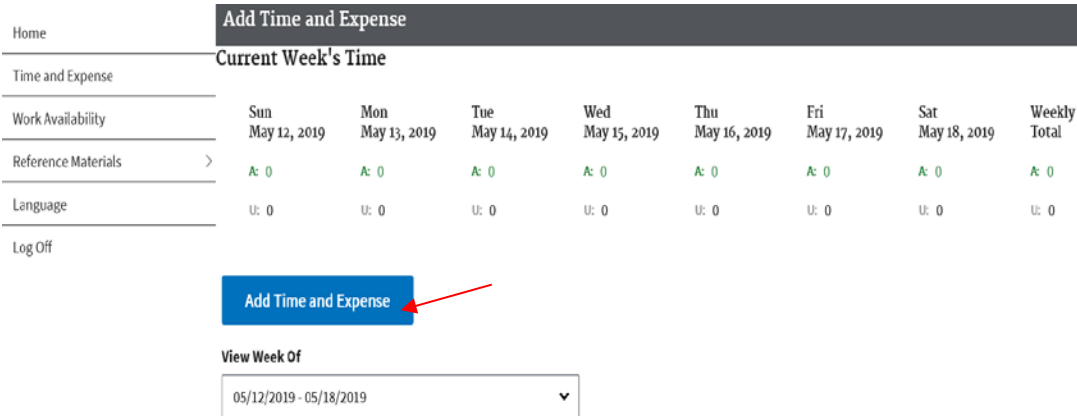
FORM D-308 (4-18-2018)		DAILY PAY AND WORK RECORD 2020 Census		U.S. DEPARTMENT OF COMMERCE Economics and Statistics Administration U.S. CENSUS BUREAU																																																									
Part A - EMPLOYEE INFORMATION																																																													
First Name		MI	Employee ID																																																										
JOHN		D	1234567																																																										
Last Name																																																													
DOE																																																													
Month		Day	Year	Day worked - Mark (X)																																																									
06		01	2020	<input type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat																																																									
1. Date worked . . .				If RECLAIM - Mark (X) this box. <input type="checkbox"/>																																																									
2. Task code . . .		Operation name . . .		Remarks																																																									
032		NRFU																																																											
3. Office code . .		Office name																																																											
2204		Providence																																																											
4. Points of travel																																																													
From		To	From	To																																																									
Home		AA + Return																																																											
Part B - PAY INFORMATION																																																													
1. Hours worked		FOR OFFICE USE ONLY		2. Times of day worked - Do not include breaks.																																																									
Regular 8.00 Training Night Differential (6 pm-6 am) Overtime Night Differential Overtime (6 pm-6 am) Sunday Premium Sunday Premium Night Differential Total 8.00		<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 25%;"> </td> <td style="width: 25%;"> </td> <td style="width: 25%;"> </td> <td style="width: 25%;"> </td> </tr> <tr> <td> </td> <td> </td> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </table>																																		<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th>START</th> <th></th> <th>FINISH</th> <th></th> </tr> <tr> <td>a. 12:00</td> <td><input checked="" type="checkbox"/> am <input checked="" type="checkbox"/> pm</td> <td>04:00</td> <td><input checked="" type="checkbox"/> am <input checked="" type="checkbox"/> pm</td> </tr> <tr> <td>b. 05:00</td> <td><input checked="" type="checkbox"/> am <input checked="" type="checkbox"/> pm</td> <td>09:00</td> <td><input checked="" type="checkbox"/> am <input checked="" type="checkbox"/> pm</td> </tr> <tr> <td>c. : </td> <td><input type="checkbox"/> am <input type="checkbox"/> pm</td> <td> : </td> <td><input type="checkbox"/> am <input type="checkbox"/> pm</td> </tr> <tr> <td>d. : </td> <td><input type="checkbox"/> am <input type="checkbox"/> pm</td> <td> : </td> <td><input type="checkbox"/> am <input type="checkbox"/> pm</td> </tr> <tr> <td>e. : </td> <td><input type="checkbox"/> am <input type="checkbox"/> pm</td> <td> : </td> <td><input type="checkbox"/> am <input type="checkbox"/> pm</td> </tr> </table>		START		FINISH		a. 12:00	<input checked="" type="checkbox"/> am <input checked="" type="checkbox"/> pm	04:00	<input checked="" type="checkbox"/> am <input checked="" type="checkbox"/> pm	b. 05:00	<input checked="" type="checkbox"/> am <input checked="" type="checkbox"/> pm	09:00	<input checked="" type="checkbox"/> am <input checked="" type="checkbox"/> pm	c. :	<input type="checkbox"/> am <input type="checkbox"/> pm	:	<input type="checkbox"/> am <input type="checkbox"/> pm	d. :	<input type="checkbox"/> am <input type="checkbox"/> pm	:	<input type="checkbox"/> am <input type="checkbox"/> pm	e. :	<input type="checkbox"/> am <input type="checkbox"/> pm	:	<input type="checkbox"/> am <input type="checkbox"/> pm
START		FINISH																																																											
a. 12:00	<input checked="" type="checkbox"/> am <input checked="" type="checkbox"/> pm	04:00	<input checked="" type="checkbox"/> am <input checked="" type="checkbox"/> pm																																																										
b. 05:00	<input checked="" type="checkbox"/> am <input checked="" type="checkbox"/> pm	09:00	<input checked="" type="checkbox"/> am <input checked="" type="checkbox"/> pm																																																										
c. :	<input type="checkbox"/> am <input type="checkbox"/> pm	:	<input type="checkbox"/> am <input type="checkbox"/> pm																																																										
d. :	<input type="checkbox"/> am <input type="checkbox"/> pm	:	<input type="checkbox"/> am <input type="checkbox"/> pm																																																										
e. :	<input type="checkbox"/> am <input type="checkbox"/> pm	:	<input type="checkbox"/> am <input type="checkbox"/> pm																																																										
3. Have you claimed ALL hours worked? If not - Please list number of hours, date(s) hours were worked, and an explanation of why you are not claiming them for payment.				Cases Completed (Filed by supervisor)																																																									
				Cases submitted																																																									
4. Reimbursements				Cases accepted																																																									
Miles driven 45		Telephone \$		\$																																																									
FOR OFFICE USE ONLY		\$		\$																																																									
Part C - CERTIFICATION																																																													
Privacy Act Notice - All information furnished will be treated in accordance with the Privacy Act of 1974. No information will be released except as authorized by the Act.																																																													
Employee's Certification - Under penalty of fine and/or imprisonment, I certify that the information on this form is true and correct to the best of my knowledge.			Supervisor's Certification - I certify that I have reviewed the entries made and they appear to be reasonable and accurate.																																																										
Signature		Date	Signature		Date																																																								
[Signature]		6/1/2020	Test One		6/2/2020																																																								
FOR OFFICE USE ONLY		Audited by (Initial and date)	Remarks		Date																																																								
					6/2/2020																																																								

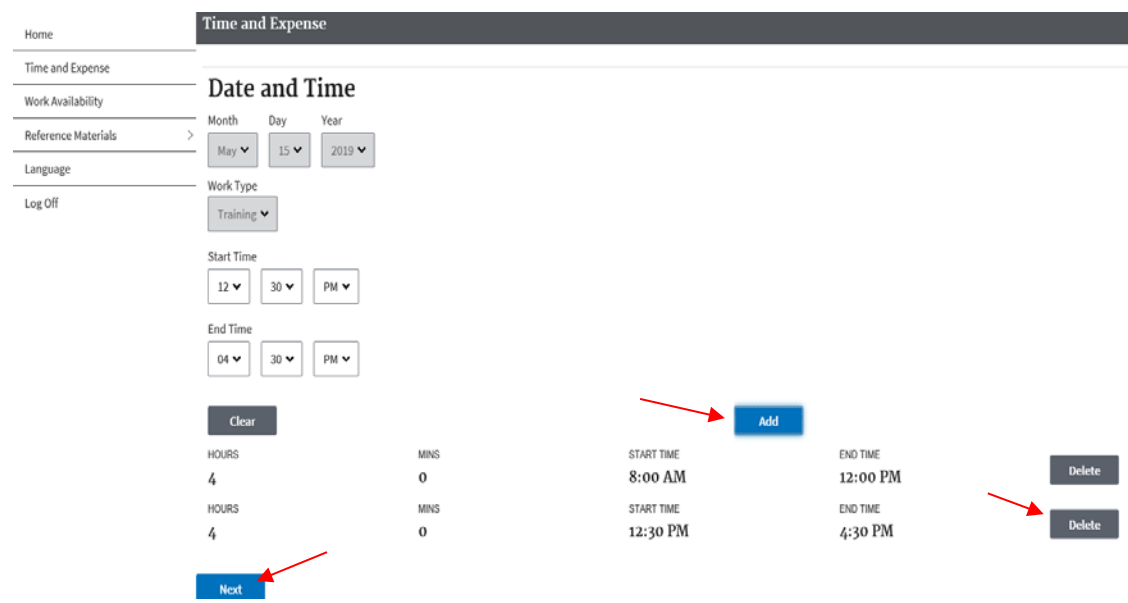
Copy distribution: ORIGINAL - Payroll COPY - Employee

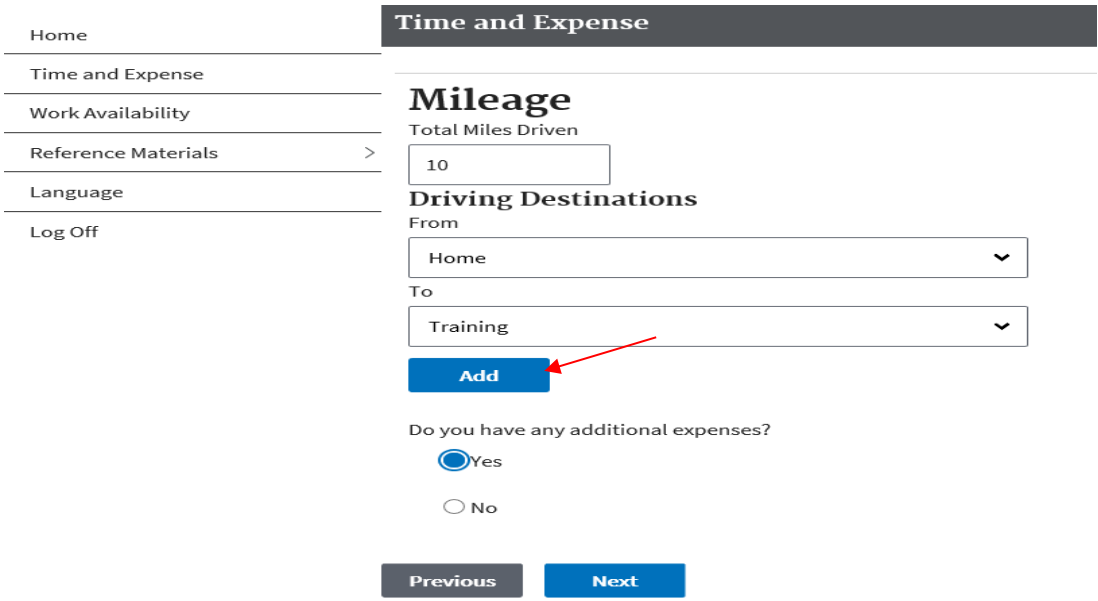
Topic 6: How to Complete Your Electronic Daily Payroll Form

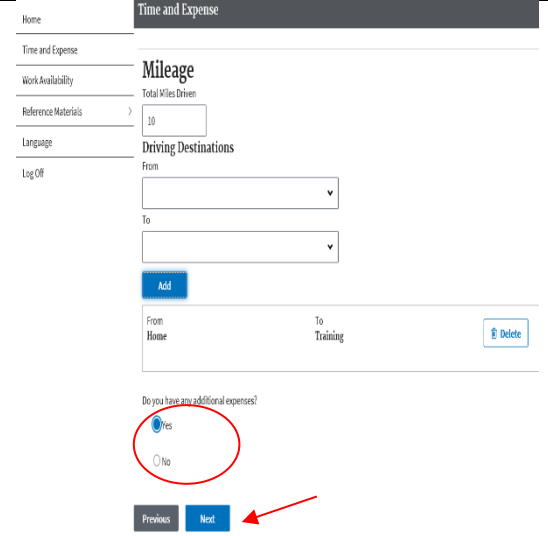
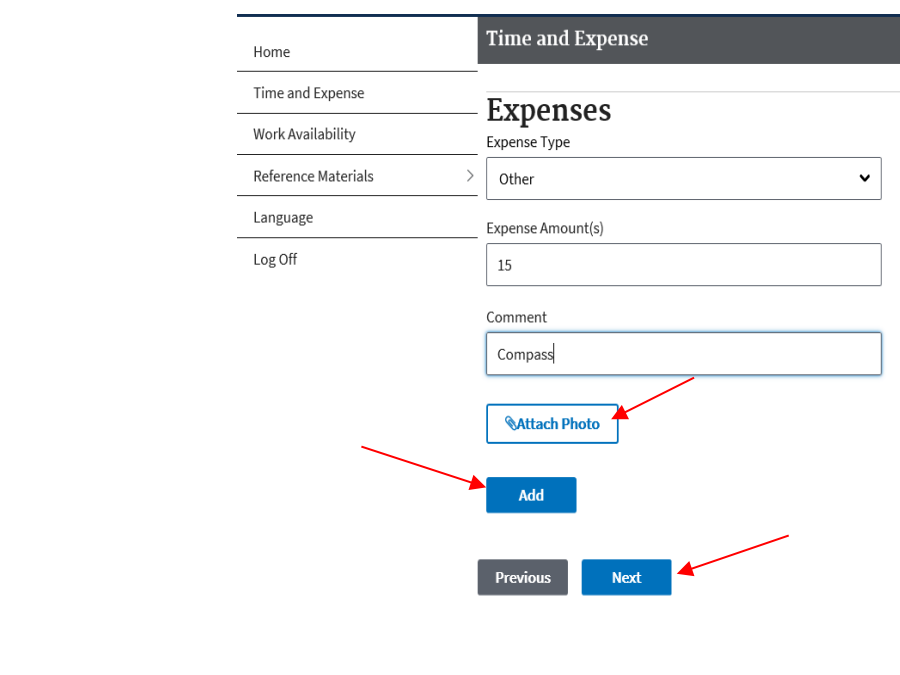
General	The Enterprise Censuses and Surveys Enabling (ECaSE) application is used to submit payroll and work availability. Complete the E-308, <i>Electronic Pay and Work Schedule</i> , and transmit for each day that you worked. There are several options you can select from the dashboard, but the two options you mostly possibly be using would be the Work Availability and Time and Expense options. Follow Figure 3-1 on how to complete your electronic payroll.
Use of Device Inside of ECaSE	The field staff (Recruiting Assistant, Census Field Supervisor, and Enumerator) and Office staff (Office Operation Supervisors and clerks) will use ECaSE to complete the E-308, <i>Electronic Daily Pay and Work Record</i> , and transmit for each day worked.
Starting New E-308	<p>The graphics and steps below explain how to enter payroll up to its approval and your validation. The steps include:</p> <ul style="list-style-type: none">• Start a new E-308• Enter your time• Enter your travel• Enter your expenses• Attach receipts, as applicable• Check the E-308 Summary• Attest and send E-308 for approval

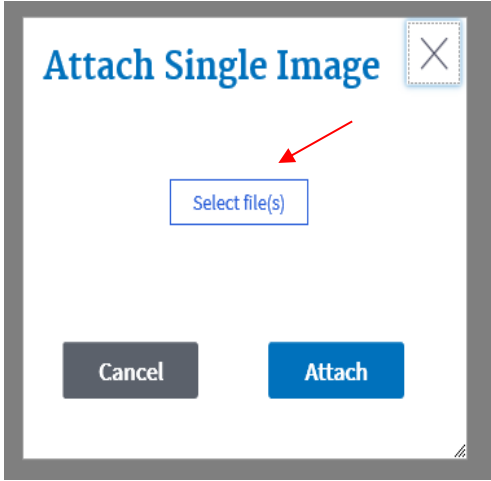
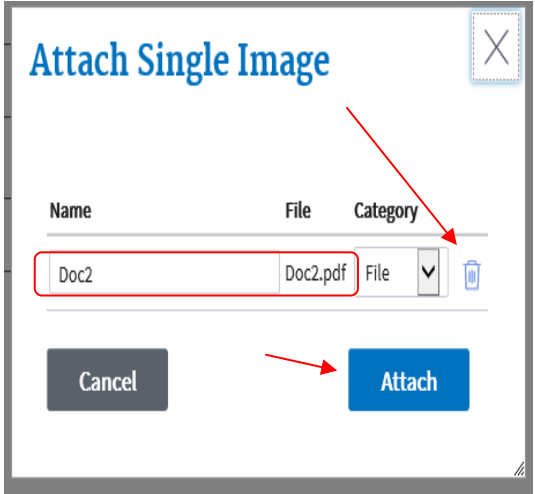
Figure 3-1: How to Complete Your Electronic Payroll

Steps	Actions	Notes
1.	Select the Time and Expenses (either of the two paths) from the dashboard.	
		
2.	On the screen titled “Current Week’s Time” click the “Add Time and Expense” button.	
		
3.	<p>Click the drop down arrows to enter the Month, Day, Year, Work Type, Start, and End times. There are 2 types of work types you can enter on this page:</p> <ul style="list-style-type: none"> Regular – Hours spent doing production work Training – Hours spent doing training in class or on-line <p>There are 2 other types of work you can choose from once you have accumulated at least 8 hours in a day or 40 hours in a week. This will be the only options for you once you have accumulated 8 hours in a day or 40 hours in a week.</p> <ul style="list-style-type: none"> Overtime – Regular, non-training, hours over 8 hours in a day or 40 hours in a week that have been approved in advance. Training Overtime – Training, non-regular, hours over 8 hours in a day or 40 hours in a week that have been approved in advance. <p>In order to enter either of the overtime work types you will first have to submit a regular hours (total of 8 hours) and attest to them, then you will have to go in and submit a new entry for the overtime hours.</p>	



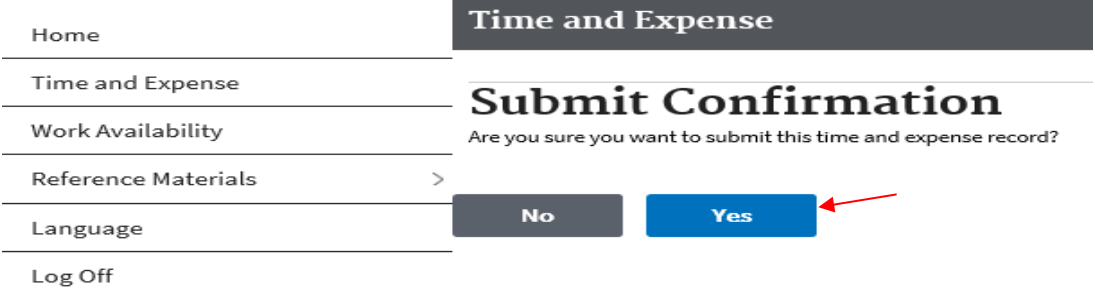
	<p>The FOCS system has edits that prevent users from entering more than 8 non-OT hours for a day and more than 40 non-OT hours for the week. If you try to do this, you will see a message indicating that and that OT needs to be submitted separately.</p> <p>For example, if users already have 6 regular hours submitted for a day (and has not submitted 40 hours for the pay week), when creating a second timesheet for the same day, the user will only see non-OT work types because they haven't hit the OT eligibility rules yet. The system will not let them enter a time window for a regular work type that is more than 2 hours. If they try to enter more than 2 hours, they will get a message preventing them from doing so. They must enter the 2 regular hours first and then submit a separate timesheet for the OT hours.</p>	
	<p>There are also 4 types of work that cannot be keyed and will automatically be calculated and put into your timesheet based on of your work date and start and end times:</p> <ul style="list-style-type: none"> • Sunday Premium - Sunday work is considered Sunday Premium and you will be reimbursed accordingly. • Sunday Night Differential - All Sunday work outside of standard business hours is considered Sunday Night Differential and you will be reimbursed accordingly. • Night Differential - All non-overtime work between 6 pm and 6 am (except on Sundays) is considered Night Differential and you will be reimbursed accordingly. • Night Differential Overtime - All overtime work between 6 pm and 6 am (except on Sundays) is considered Night Differential and you will be reimbursed accordingly. <p>You will not need to key in a total number of hours worked, the system will calculate this based off of the time frame you enter (ie. 9:00 AM – 10:00 AM will be considered 1 hour). Once all data has been entered click the add button. The time entry has now been submitted and can be seen at the bottom of the page.</p>	
		
4.	<p>If you need to enter in multiple time frames for the day you worked (i.e., 9:00am – 10:00am and 12:00pm – 3:00pm on 5/21/2017) you</p>	<p>Once entries are added, all entries for the current date will be displayed at the bottom of the page.</p>

	<p>may do so by entering a new start time and end time and clicking the Add button.</p> <p>If you need to delete a specific time entry click the Delete button next to the desired entry. Once all time frames have been entered click the Next button.</p> <p>If you need to enter multiple work types (regular, training, overtime, or training overtime) for one day you will need to submit the hours for each work type separately. Only one work type can be used per entry; however, you can add up to four time intervals entry in a single work day. For example, you can input and submit 4 hrs. Regular, 3 hrs. Training, then enter an hour work time after 6 p.m. to 6 a.m., considered as ND, and then enter and submit an entry for OT or ND OT for that same day.</p>	<p>You will see these hours again on the attest screen before you certify or submit your timesheet.</p> <p>Selecting the Next button will prompt the system to move to the Mileage page.</p>
5.	<p>Enter any mileage you may have in the "Total Miles Driven" field. If you claim miles you must enter where you drove from and to. Enter this in the "From" and "To" fields. Entries of Home, Assignment, Training, Meeting, or Other are all acceptable for these fields. Once you have entered in the data click Add.</p>	<p>Mileage reimbursement does not include any mileage driven detouring from employee's assignment for any non-work-related activity such as lunch, stopping by at WalMart, and so on. Once the mileage is added, the data will be displayed below the page, and you have the option to delete the file if necessary, or select the Next button to move to the Expense page.</p>
		
6.	<p>If you need to add additional mileage entries then click the Add button and repeat step 5.</p>	<p>If the 'Other' is selected, a new 'From Location' and 'To' fields will appear and you must enter your traveled locations. On these fields, you can be precise of your whereabouts unlike in</p>

		<p>manual Form D-308, due to its limited space. You may include the city, county, and state, of your travels, e.g., your work starts in Potomac, MD (Montgomery County) and you traveled to Great Falls, VA (Fairfax County), throughout the day to pick an item needed for the training. The maximum characters that can be entered in each field is 50.</p> <p>If you have additional expenses click the “Yes” radio button then click the Next button. If no additional expenses click the “No” radio button then click Next to move to the Expense page.</p>
7.	<p>Enter additional reimbursable expenses using the Expense Type drop down menu. The following expenses can be found in the Expense Type drop down menu: Parking, Public Transit, Tolls, and Other.</p>	<p>You must enter a remark in the Comment box whenever you selected the “Other” expense. Explain what the expense is for, e.g., phone call, purchase of a map, etc. The system allows up to five expenses to be added.</p>
		
8.	<p>The <u>Attach Photo</u> button will automatically appear for attachment of receipt for any expense(s) entered that costs five (\$5) dollars or more. To add a photo of a receipt click the “Attach Photo” button. You will then be prompted to attach an image. Click the “Select files” button.</p>	<p>Attaching receipt varies slightly by the device that is being used, i.e., Smartphone versus Tablet.</p> <p>The system will not move forward if no attachment of receipt is included for a \$5 or more expense.</p>

<p>9.</p>	<p>You will then be prompted to search for the image you wish to attach.</p> <p>***Only jpg, jpeg, png, and pdf files, and not to exceed 2 megabytes are allowed to be attached. You'll receive an error message if the file is not within the requirement.***</p> <p>After you have selected the file you wish to attach, you may select the Delete button if you selected the wrong file; otherwise, click the "Attach" button. The file attachment will be displayed below where employees have the option to view or delete it. Once attachment is validated and no changes to be made, click on the Add button to add it to the time and expense record. You have the option again to delete the file, if necessary.</p>
	<div style="display: flex; justify-content: space-around;">   </div>
	<div style="display: flex;"> <div style="flex: 1;"> <p>Home</p> <hr/> <p>Time and Expense</p> <hr/> <p>Work Availability</p> <hr/> <p>Reference Materials ></p> <hr/> <p>Language</p> <hr/> <p>Log Off</p> </div> <div style="flex: 2;"> <div style="background-color: #444; color: white; padding: 5px; text-align: center;">Time and Expense</div> <h2 style="margin-top: 10px;">Expenses</h2> <p>Expense Type</p> <div style="border: 1px solid #ccc; padding: 5px; display: flex; justify-content: space-between;"> Other ▼ </div> <p>Expense Amount(s)</p> <div style="border: 1px solid #ccc; padding: 5px; width: 100%;">15</div> <p>Comment</p> <div style="border: 1px solid #ccc; padding: 5px; width: 100%;">Compass</div> <div style="display: flex; justify-content: space-around; margin-top: 10px;"> <div style="border: 1px dashed #ccc; padding: 5px; text-align: center;"> </div> <div style="border: 1px solid red; padding: 5px; text-align: center;"> </div> </div> <div style="text-align: center; margin-top: 10px;"> <div style="background-color: #007bff; color: white; padding: 10px 20px; display: inline-block;">Add</div> </div> <div style="display: flex; justify-content: center; margin-top: 10px;"> <div style="background-color: #444; color: white; padding: 5px 15px; margin: 0 10px;">Previous</div> <div style="background-color: #007bff; color: white; padding: 5px 15px; margin: 0 10px;">Next</div> </div> </div> </div>

<p>10.</p>	<p>The saved data will be displayed below where you have the option to delete it, if necessary, by selecting the Delete button. If you need to add multiple expenses for the day then repeat these steps by clicking the Add button until you have entered all authorized expenses. After all expense data has been entered click the Next button to move to the Summary page.</p>	
<p>11.</p>	<p>You will see a summary of all the time and expenses you have entered for this date. If you had hours worked that fell under a premium pay category then you will see the hours that were converted here, too. Use this summary to review your timesheet.</p> <p>The <u>Summary</u> tab is pre-selected for you to view, and the <u>Expenses</u> tab allows you to also view your expenses summary information.</p>	<p>It is very important that you check the information in the E-308 before you submit it. After you verified the information and everything is correct, select the Next button to move to the Attest page.</p>

12.	<p>You will then be asked to attest that the information on the form is true and correct. Click the “I agree to the terms above” check box (you will not be allowed to attest your time and expense data if this box is not checked), then click the “attest” button.</p>
	<div style="display: flex; justify-content: space-around;"> <div style="width: 45%;">  </div> <div style="width: 45%;">  </div> </div>
13.	<p>You will then be asked if you want to submit the final payroll record for the day, if so click the “Yes” button.</p> <p>After selecting the “Yes” button, the system will move your time and expense to the History screen.</p>
	
	<p>You have now submitted your timesheet to your supervisor for approval. Your supervisor can either approve or reject your timesheet. Your timesheet can have one of the following statuses:</p> <p>TRANSMITTED-PENDING – Submitted to you supervisor but has not been approved or rejected.</p> <p>ACCEPTED - Submitted to you supervisor and has been approved.</p> <p>REJECTED - Submitted to you supervisor and has been rejected.</p> <p>NOT ATTESTED – Timesheet has not been attested</p> <p>NOT TRANSMITTED – Timesheet has not been transmitted</p> <p>If your supervisor rejected your timesheet you will need to resubmit your timesheet in order to be paid for your time. Your supervisor will put a comment at the bottom of your timesheet explaining why they rejected it. Once you have fixed the issue with your new timesheet you can then resubmit it for approval.</p> <p>You may select the Add Time and Expense button, to add a new work hours and/or expenses for the pay period, if applicable. Otherwise, select the Log Off to log out from the ECaSE application.</p>

Home
Time and Expense
Work Availability
Reference Materials
Language
Log Off

Add Time and Expense
Current Week's Time

Sun May 12, 2019	Mon May 13, 2019	Tue May 14, 2019	Wed May 15, 2019	Thu May 16, 2019	Fri May 17, 2019	Sat May 18, 2019	Weekly Total
A: 0	A: 0	A: 0	A: 0	A: 0	A: 0	A: 0	A: 0
U: 0	U: 0	U: 0	U: 8	U: 0	U: 0	U: 0	U: 8

Add Time and Expense
View Week Of
05/12/2019 - 05/18/2019

Date	Total Time Worked	Miles
5/15/19	8	10
STATUS TRANSMITTED-PENDING		

If you selected No, your data will be saved and you may submit it at a later time by clicking the **Submit** button. Your timesheet status will display as Not Transmitted.

Home
Time and Expense
Work Availability
Reference Materials
Language
Log Off

Time and Expense
Submit Confirmation
Are you sure you want to submit this time and expense record?
No
Yes

Home
Time and Expense
Work Availability
Reference Materials
Language
Log Off

Add Time and Expense
Current Week's Time

Sun May 12, 2019	Mon May 13, 2019	Tue May 14, 2019	Wed May 15, 2019	Thu May 16, 2019	Fri May 17, 2019	Sat May 18, 2019	Weekly Total
A: 0	A: 0	A: 0	A: 0	A: 0	A: 0	A: 0	A: 0
U: 0	U: 0	U: 0	U: 0	U: 0	U: 0	U: 0	U: 0

Add Time and Expense
View Week Of
05/12/2019 - 05/18/2019

Date	Total Time Worked	Miles
5/15/19	8	10
STATUS NOT TRANSMITTED		

Submit

Topic 7: Submission of Paper Payroll Documents

When to submit payroll documents

Turn in a completed payroll document (*when applicable*) to your supervisor each day you worked. If you have a document to submit but will not be working the next day, notify your supervisor of your absence and turn in the form the next day you report for work. If you work in rural areas and your supervisor concurs that it is counterproductive to submit a form each day make arrangements with your supervisor to submit documents as soon as possible. If you do not meet with your supervisor daily, turn in forms for work completed on Friday, Saturday, and Sunday on the following Monday unless special arrangements have been made.

Review and certification of payroll documents

Your supervisor will review all your payroll documents (*when applicable*) and, if needed, make changes or corrections. Make sure your work justifies the hours you claim. Each payroll document you submit must show your signature and your supervisor's signature, along with the date the document is signed. ***Documents will not be processed without the required signatures and date.***

Distribution of payroll documents

Review your payroll form with your supervisor. After your supervisor verifies and signs your payroll document, remove the *employee copy* and give the original to your supervisor. Your supervisor will forward them to the payroll office for payment processing. Keep your employee copies in a safe place until you receive an earnings statement and paycheck for that pay period. This way, you can compare your copies to your earnings statement. Report any discrepancies to your supervisor.

Topic 8: Disallowances and/or Reclaims for Paper Payroll Forms

General

Occasionally, hours or claims for reimbursement will not be paid for lack of proper explanation or required receipts. A copy of your payroll document, D-308, will be returned to you showing the disallowance. You can reclaim the disallowance and attach any supporting documents by following the steps in Table 3-4.

Table 3-4: Submitting a reclaim

STEP	ACTION
1	Prepare a new D-308 with the same identifying information as shown on the original claim, including the same work day.
2	Put an X in the RECLAIM box.
3	Enter only the information for the hours or expenses being reclaimed.
4	Attach any receipts or other required supporting documentation that were not previously submitted.
5	In the Remarks section of the payroll document, enter the phrase "Reclaim of (enter hours, amount, etc.) disallowed in pay period ending (give date) due to (give reason). Correct documentation submitted with this reclaim where applicable."
6	Sign the RECLAIM document and give it to your supervisor for approval. Keep the employee copy for your records. <i>Forms cannot be processed without the required signatures and date.</i>

Review and certification of RECLAIM payroll documents

Your supervisor will review all of your RECLAIM payroll documents and, if needed, make changes or corrections. Each RECLAIM document you submit must show your signature and your supervisor's signature, along with the date the document is signed. Documents cannot be processed without the required signatures and date.

Distribution of RECLAIM payroll documents

After your supervisor verifies and signs your RECLAIM payroll document, remove the employee copy and return the original to your supervisor. Your supervisor will forward them to the payroll section for processing. Keep your copy in a safe place until you receive an earnings statement and paycheck for the reclaimed amounts. This way, you can compare your copy to your earnings statement. Report any discrepancies to your supervisor.

Topic 9: Fraudulent Claims Against the United States

Fraudulent claims

Your claims for hours and reimbursement of associated expenses should accurately reflect the time and costs relating to your official duties so that you might avoid any violations or apparent violations of the law. Your claims may be forfeited if you attempt to defraud the government in connection with any expenses. Fraudulent claims will result in termination of employment. Additionally, there are criminal provisions under which severe penalties may be imposed if you knowingly present a false, fictitious, or fraudulent claim against the United States.

Topic 10: Designation of Beneficiary for Unpaid Compensation of Deceased Civilian Employees

Unpaid compensation

The SF-1152, *Designation of Beneficiary*, is used to designate payment of death benefits. It applies to any money due the employee at the time of death, such as unpaid salary. An employee may complete this form during their employment, to change the normal order of payment of death benefits listed on the form. You may obtain this form from your supervisor.

If there is no designated beneficiary living, any unpaid compensation that becomes payable after the death of an employee will be payable to the first person or persons listed below who are alive on the date entitlement to the payment arises.

1. To the widow or widower.
2. If neither of the above, to the child or children in equal shares, with the share of any deceased child distributed among the descendants of that child.
3. If none of the above, to the parents in equal shares or the entire amount to the surviving parent.
4. If there are none of the above, to the duly appointed legal representative of the estate of the deceased employee, or if there be none, to the person or persons determined to be entitled thereto under the laws of the domicile of the deceased employee.

You do not need to designate a beneficiary unless you wish to name someone not included above, or in a different order.

Topic 11: Employment Resolution Contact

Reporting employment problems

If you encounter problems of any kind relating to your employment at the Census Bureau, contact your Regional Census Center at 855-236-2020, option #3.

Chapter 4: Travel Expenses

Topic 1: General

General

Most of your census assignments are conducted in or around the area in which you live. However, there may be occasions when you might be asked to travel and stay at least one night to conduct census activities. In these cases, you will be reimbursed for per diem expenses.

Non-Local Travel Claims for DAPPS Employees

Field and office intermittent employees paid weekly by the Decennial Applicant, Personnel, and Payroll System (DAPPS) will have their official non-local travel expenses recorded in the E2Solutions (E2). E2 is a web-based end-to-end travel and expense management tool. It offers traveler a convenient and user-friendly way to create and track traveler's travel authorizations, get approvals, submit vouchers, receive reimbursements and book travel reservations.

If you need to go on official non-local travel, the Area Census Office will notify you. The office will create your user profile and arrange your travel in E2 solutions. Once your travel arrangements have been recorded in E2 Solutions, you should receive your itinerary in the mail. Intermittent employees will be responsible to save all appropriate receipts pertaining to the travel. Once travel is complete, please send a copy of your receipts to the Area Census Office administrative area for processing.

Your reimbursements for expenses claimed will be either deposited in the account you indicated or a check will be mailed based on your preference you selected on the form D-1199.

Local Travel Claims

Local travel is defined as travel that:

- Is completed within one calendar day of 12 hours or less,
- Does not involve overnight lodging, and

- Is generally limited to points within a 50-mile radius of the official duty station or residence

Local travel will always be recorded on your E-308 or if necessary a D-308.

Note: Treat travel to worksite that is greater than 50 miles as local travel as long as the travel status does not exceed 12 hours and does not require lodging or use of rental car.

Although a travel order is not required for local travel, supervisors must give the traveler verbal approval.

Allowable expenses for local travel include:

- Privately-Owned Vehicle (POV) mileage. POV includes automobile, motorcycle, and airplane. **Note:** Employees cannot claim for miles traveled from the employee's residence to the official duty station
- Parking fees for POVs
- Toll and bridge fees
- Taxi fares
- Fees for public transportation (bus, subway, and so on)
- Official business telephone calls made from cellular or pay phones
- Miscellaneous expenses (must be explained in detail)

Authorization for overnight travel

The Area Manager, and/or the Area Census Office Manager (ACOM), and Regional Director (or designee) at the Regional Census Center (RCC) must authorize all overnight travel. Proper documentation indicating approval will be given to you. Do not conduct overnight travel without official authorization or reimbursement will not be allowed.

Topic 2: Per Diem Expenses

Per diem expenses

Per diem is a fixed amount paid under specifically authorized circumstances to cover certain out-of-pocket expenses incurred while on official duty away from home overnight. Per diem expenses include fixed allowances for —

- Meals and incidental costs such as tips and minor costs associated with your stay
- Lodging costs

Authorization of Per diem

Per diem is authorized on your *Travel Order*. Travel orders are completed by the ACO in E2. In the event that you are authorized per diem, your office will provide you with instructions.

Per diem rate limitations

The General Services Administration (GSA) sets per diem rates for lodging, meals, and incidentals. Amounts are set according to the cost of living within each state and U.S. territory.

It is your responsibility to locate a lodging facility that is within the limit of the preset amount. The amount you receive is usually enough to cover 100% of your expenses. If lodging costs more than the fixed amount allowed, you must seek authorization from the RCC to cover the excess amount **before** your travel begins. If pre-authorization is not sought, then you may be responsible for the difference.

The per diem allowance for each travel day is established on the basis of the actual amount the traveler pays for lodging plus an allowance for meals and incidental expenses (M&IE), the total not to exceed the applicable maximum per diem rate. Travelers receive payment of three quarters or 75% of the applicable M&IE rate on the first and last days of travel. For example, in San Joaquin County where M&IE is \$44 a day, on the first and last day of travel an employee would receive \$33.

The Area Census Office (ACO) will provide travelers the maximum daily per diem rates allowed for each destination. Do not exceed these amounts. See your supervisor or ACOM for specific rates before you make arrangements.

Personal telephone calls

A daily allowance of up to \$5 is provided for personal telephone expenses except on the last day of travel. The ACOM must approve expenses exceeding \$5. However, employees are expected to limit phone calls to a reasonable duration and frequency. Approving officials shall have the authority to disallow claims that appear excessive.

We're Census bound in 2020!!



Remember - All overnight travel must be authorized by the Area Manager and/or the Area Census Office Manager (ACOM) and the Regional Director at RCC prior to traveling.

Have a safe journey

This Page Intentionally Left Blank

Chapter 5: Personal Safety and Security

Topic 1: Coverage

General

Your personal safety is of utmost importance to the Census Bureau. We value you as much as the work you do. Without you there would be no census!

Always be safety-minded and conscious of your work surroundings. Make sure you heed all regulations pertaining to fire hazards, obstructions of views and passageways, and the proper operation of small and large equipment. Census work is not hazardous, but you must observe certain safety precautions, as in any job. All accidents and injuries referred to in this chapter relate to those occurring within the scope of your Federal employment.

Accident and injury coverage

If you sustain bodily injury or are in a vehicular accident while on official census duty, under the Federal Employees Compensation Act you are entitled to immediate first-aid care and full medical care including hospitalization. There is no cost to you.

Additional benefits apply for loss of earning capacity, permanent partial disabilities, permanent total disabilities, and death. This benefit carries with it your responsibility to return to duty as soon as you are released to perform any useful work. If you are not able to immediately return to your regular job, Census may design a temporary special-duty assignment for you. You will receive regular wages and benefits for this temporary assignment.

Assault coverage

Under federal law, you are protected against verbal and bodily assaults and attacks. Title 18 of the United States Code prohibits persons from intimidating or assaulting census employees while conducting census activities in the field.

Legal actions

Public Law 87-258, Title 28 of the United States Code, Section 2679, provides that the Attorney General shall defend any civil action brought in any court against any employee of the government for damage to property or for personal injury, including death, resulting from the operation of any motor vehicle

by the employee while acting within the scope of his or her employment, that is, performing official government business.

If any legal actions are brought against you for any reasons while acting within the scope of your employment, advise your supervisor immediately.

**Prohibited Possession
of Weapons and
Chemical Projectors**

The Census Bureau does not condone, encourage, or otherwise allow field employees to carry firearms or other weapons while performing their official duties. The Census Bureau does not officially allow employees to carry pepper spray or other chemical projectors while on official government business. If an employee chooses to carry any chemical projectors that is permissible by local law and an individual owns and carries a commercially available products that is an employee's personal decision. The use of any such device will be a personal decision with any criminal or civil liability accruing to the employee. The Census Bureau does not support or represent an individual as an employee performing official duties in a case involving the use of a chemical projector.

Topic 2: Safety

General

If you use your vehicle for official census duty, you must have vehicle insurance that will cover any injuries and damages received and/or caused by you in cases of accidents.

The federal government will not reimburse you for damages to your vehicle and any injuries or damages to vehicles and their occupants caused by you. Before leaving for an assignment, inform a family member or neighbor of the general location of your assignment and the time you expect to arrive home. Do not specify the exact location as this is confidential information.

Safety when walking alone

The following advice is offered by experienced census employees. Most is plain common sense but sometimes we are not conscientious about these details.

- **Never text or use electronic devices while walking. This practice dramatically increases the likelihood that you will trip or fall.**
- Stay on well-lit streets when walking at night. Avoid walking past dark shadows near buildings, or walking too close to doorways, shrubbery, and other potential hiding places. If needed, use a flashlight.
- **Be aware of weather conditions:**
In hot weather, drink water and stay hydrated. Know the warning signs of heat exhaustion: dizziness, headache, muscle cramps, etc. Get help immediately, if you notice any of these signs. Dress appropriately in cool clothing and find shade, if needed.
In cold weather, stay hydrated, keep extremities covered and pay attention to icy surfaces; be alert for 'black ice.' Walk slowly and take small steps.
- Carry handbags close to your body, with the flap or clasp next to you.
- Be cautious when riding elevators. If you are suspicious of another passenger, wait for the next car.
- Carry wallets in an inside or front pocket to avoid pickpockets.
- Avoid walking on uneven, broken, or poorly constructed surfaces or stairs.

- Grasp the handrails along stairways. If one is not provided, proceed with extra caution.
- Wear comfortable easy-walking shoes. These shoes may come in handy should there be a need to run.
- Do not carry valuables, such as large sums of money, expensive jewelry, and watches.
- When entering a building, pause and let your eyes adjust to the indoor lighting before moving on
- Stay alert for objects that may pose tripping hazards.
- Be aware of your surroundings at all times.

Safety when traveling in your vehicle

Please heed these tips when traveling in your vehicle:

- Never pick up hitchhikers in your vehicle.
- Watch for erratic movements of other cars. **Drive defensively**, yielding to other cars to avoid accidents.
- Check your maps and locations before you start to drive. If necessary, pull off the road into a parking lot and stop your vehicle to check directions. **Never use GPS (unless the GPS navigation is hands-free and hands-free usage is permitted by the law of the state in which you are driving) or other electronic devices while driving.**
- Observe speed limits.
- **It is mandatory to wear a seat belt at all times, even when pulled to the side of the road. This requirement remains in force regardless of any individual state or tribal law.**
- Keep your doors locked.
- Watch for children, jaywalkers, and pedestrians.
- Keep your vehicle in good operating condition with emphasis on brakes, lights, tires, wiper blades, and belts.
- Park in well-lit parking places at night.
- As you walk towards your vehicle, scan beneath the vehicle for persons waiting to charge out at your ankles. Check the back seat and floor for hidden persons before entering your vehicle.
- If your vehicle stalls, stay inside and hang a brightly colored cloth out the window. If someone stops to assist you, stay in the vehicle and ask the person to phone the police for help.

- If you are being followed, do not drive directly home. Drive to the nearest police or fire station, hospital, or other public place. Do not exit your vehicle until it is visually safe.
- Have your vehicle keys ready before you reach your car. Do not open your purse or distract yourself when walking to your vehicle.
- Maintain a safe distance from the vehicle ahead of you. Don't tailgate.
- **Do not use cell phones, handhelds or other such devices while driving. Pull off of the road into a parking lot. When the car is in motion, pay 100% attention to your driving.**
- Check for other vehicles before backing, turning, or entering an intersection.
- Do not carry valuables in your car; keep your car locked when parked.
- Watch for deer, moose and other animals in rural areas.
- Be alert to brake lights or turn signals beyond the vehicle ahead of you. Anticipate when others will slow down.
- When stopping, leave space between you and the vehicle ahead of you. Should another vehicle rear-end you, this may protect you from hitting the car in front.
- Drivers operating motorcycles to conduct Census business are required to wear helmets at all times, regardless of individual state or tribal law.

Safety from pets and other animals

Although some pets may be friendly, not all are friendly towards strangers. If you come into contact with pets or other animals, consider the following tips:

- Obey the signs displayed in respondents' yards. If you observe a "Beware of Dog" sign, take extra precaution.
- If warning signs are posted, try to call the respondents to the door before entering the premises.
- Do not run past a dog. The dog's natural instinct is to chase and catch prey.
- If confronted by a dog, face the dog without making direct eye contact and back away slowly. Be submissive, but don't run. If you run, the animal might try to knock you to the ground and you could be seriously hurt.

Put something between you and the dog, such as a bag. Do not try to make friends with the dog, don't try to pet the dog, and don't put your hands or face near it. If the dog does bite you, don't pull away – it will cause a tear and a worse wound. Instead, try to make the dog release its hold.

- Many dog bites occur inside respondents, homes. If you encounter a dog inside, ask respondents if they would mind confining the dog to another room during the interview.
- Learn to recognize the warning signs that a dog is about to attack; tail high and stiff, ears up, hair on back standing up, and teeth showing.
- If a bite or scratch from a dog or other wild or domestic animal breaks your skin, consult your doctor or an emergency room about the advisability of receiving rabies inoculation or other medical treatment.

Contact your supervisor for instructions if you consider an area too unsafe for you to work in.

Face Covering is Mandatory

As part of our ongoing efforts to keep employees and the general public safe, face coverings are now mandatory. Field Division requires that all employees wear face coverings that cover your nose and mouth while interacting with fellow employees, the public, and while conducting field operations. According to the CDC, face coverings help decrease the spread of COVID-19. If you have any concerns regarding your ability to comply with this directive, please contact with your immediate supervisor as soon as possible.

The requirement for face coverings does not supersede or substitute the previously established COVID-19 guidance that you received. Therefore, you are required to wear face coverings if you are not 6 feet away from others, avoid contact with people who are sick, and wash your hands often with soap and water or hand sanitizer. A failure to comply with the directive to wear face coverings and/or adhere to any other established COVID-19 guidance may result in administrative action, up to and including, termination.

Additional Guidelines

- For your safety, employees should remove their face covering while driving between assignments.
- By wearing a face covering, you are letting all staff around you and the American public know you “have them covered” and this personal protective item represents one of the most effective ways to protect each other.

Face Mask Graphic

Below is the face mask graphic which provides important information on how to properly wear and remove a face mask as well as some helpful health and sanitization tips while using a face mask.

How to Wear a Cloth Face Mask

Here are a few tips for wearing and removing a cloth mask:

- Wash or sanitize your hands before wearing.
- Mask should cover the nose, mouth, and chin.
- Tie it behind your head or use the ear loops and ensure it is snug.
- Avoid touching the mask while wearing.
- If the mask is touched, wash or sanitize your hands immediately.
- While untying, avoid touching the front of the mask.
- Wash your hands immediately after removing.
- Regularly launder your mask. You can also launder it with your other clothes.

Finally, here are a few face mask precautions:

- Do not put masks on anyone who has trouble breathing, is unconscious, or otherwise unable to remove the mask without assistance.
- Do not use face masks as a substitute for social distancing.



For the latest updates on the COVID-19 pandemic, check the **Centers for Disease Control and Prevention Web site** and [mayoclinic.org](https://www.mayoclinic.org).



U.S. Department of Commerce
U.S. CENSUS BUREAU
[census.gov](https://www.census.gov)

Topic 3: Vehicular Accidents

What to do if you are involved in a vehicular accident while working

In case of a vehicular accident while working, do the following:

- If you sustain injuries, seek medical attention and contact your supervisor as soon as possible for guidance.
- If you require medical attention, contact the Area Specialist for Workers' Compensation (ASWC) at 1-800-819-4215 and the Administrative Specialist at the Regional Census Center (1-855-236-2020, option #3) as soon as possible. The ASWC will authorize treatment by faxing a form to the attending physician. The ASWC will email instructions to the injured worker to register an account in ECOMP, report the injury on an OSHA 301 form and file a Workers' Compensation claim, all through the electronic ECOMP system. Please be prepared to provide physician information.
- Exchange names, addresses, and driver license numbers with the other involved party. **Do not** sign your name on anything. This is to protect you from fraudulent statements prepared by someone else without your knowledge.
- Wait for a law enforcement officer to come on the scene before discussing the accident. It is not wise to make statements or give opinions to someone other than a law enforcement officer.
- Look for witnesses to the accident. Exchange names and addresses with the witnesses. Give each one a SF-94, *Statement of Witness* to complete. If a witness is unable to complete the report at the scene, ask that it be completed later and mailed to your home or the Area Census Office (ACO). Give the address of the ACO. *(One SF-94 is contained in Appendix A. Copy it as needed. If more than one witness, mail a copy of the form to the witness as soon as feasible. Have the witness mail the completed form to your home or the area census office address. If your handbook is in a PDF version, you will need to call the ASWC for a copy of the form(s))*
- While waiting for a law enforcement officer to appear on the scene and if serious bodily injury is not sustained, fill out a SF-91, *Motor Vehicle Accident Report* in its entirety. If you cannot complete it immediately after the accident occurs, then do so as soon as possible so as not to forget

the important details. *(One SF-91, Motor Vehicle Accident Report is contained in Appendix A. Copy it as needed. If your handbook is in a PDF version, you will need to call the ASWC for a copy of the form(s))*

- Notify your supervisor of your accident as soon as possible.
- Within 48 hours of the accident, give your supervisor a copy of all completed witness statements, the SF-94, and your accident report, the SF-91, and include copies of any citations, tickets, subpoenas, or summonses you might have received as a result of the accident. If a police report is issued, be sure to obtain any “key” or explanation of codes used in the report. Provide copies of both to the RCC.
- Complete the required accident report forms provided by **your own insurance company**.
- If you receive accident report forms from other insurance companies, contact your insurance company and office to learn of your obligation, if any, in completing them.

**Instructions for
completing the SF-91,
Motor Vehicle Accident
Report**

Use these instructions to complete the SF-91.

Items 1-11: Enter information about you and your vehicle. Item 4a would be the ACO address. For Item 6 do not wait for an estimate, that can be submitted later.

Items 12-25: Enter information about the other vehicle involved in the accident. If more than 1 other vehicle was involved provide the information about that vehicle(s) on a separate sheet of paper or in Section VIII.

Items 26-46: Record information for all injured persons including yourself, if applicable. If more than 2 people were killed/injured provide that information on a separate sheet of paper or in Section VIII. If no pedestrians were involved leave Item 46 blank.

Items 47-52: Enter information regarding the accident. In Items 50 and 52 label the vehicles as shown. Your vehicle is considered the *Federal* vehicle.

Items 53-62: Provide the information for witnesses given a SF-94, *Statement of Witness*.

Items 63-67: Enter information on property damage. If no property was damaged, leave this section blank.

Items 68-70: Enter the police information

Item 71: Sign and date the form.

Items 72-80: Enter the details of your trip.

Items 81-88: Leave blank. This will be filled out at the RCC.

**Extended delay from
returning to duty**

If you are delayed from returning to duty due to injuries sustained from your accident, it is your responsibility to promptly provide medical documentation specifying in detail the nature of your disability. If alternate duties are offered to you to perform until you are fully recovered, you are generally required to accept them. Contact the ASWC and Administrative Specialist to discuss particulars regarding the Workers' Compensation Program.

Topic 4: Personal Injuries

What To Do In Case of Accident and/or Injury

1. INJURY AND WORKERS COMPENSATION REPORT

In cases of an accident and/or injury, the employee will contact the ASWC by calling the ARE YOU HURT number at 1-800-819-4215 and select the prompt for their respective region. They will also contact the Administrative Specialist (safety) at the RCC. When appropriate, the ASWC will authorize treatment by faxing a form to the attending physician. **The ASWC will email instructions to the injured worker to register an account in ECOMP, report the injury on an OSHA 301 form and file a Workers' Compensation claim, all through the electronic ECOMP system.** When the ASWC is notified by an employee that an accident/injury occurred, the ASWC will email the Administrative Specialist (safety) and ACOM with the employee's name, date of injury and brief description of accident.

The Census Field Manager should receive notification from the supervisor that an injury occurred. If an employee calls the ACO directly regarding an accident/injury, refer the employee to the ASWC's toll-free number (1-800-819-4215); if the employee is in immediate need of medical treatment, instruct them to seek treatment first and contact the ASWC immediately afterward.

2. REMEDY CASE MANAGEMENT REPORTING

In the case of an injury, the employee must also report the injury by calling the Decennial Service Center, at (855) 236-2020, selecting option #1 and report the incident to the Remedy Case Management (RCM) Incident Reporting System (RCM).

Once the incident is reported to RCM, it will be assigned for a member in the Office of Security (OSY) to investigate. The incidents should be reported immediately. The purpose of the immediate time-frame is to provide details while events are fresh and can be more accurately recalled. Immediately reporting the assault may also increase the possibility of recovering property, and a timely apprehension of the perpetrator.

RCM process:

1. Call the Decennial Service Center, Toll free at 1-855-236-2020, and choose Option 1.

2. An analyst will take the report and enter it into RCM by asking a series of pre-defined questions designed to obtain information about the incident.
3. The RCM system will generate automatic notifications to the office(s) with a need to know based on the information collected.
4. The affected office(s) will begin their investigation, which will include following up with the employee who reported the information.

Note: If there is any law enforcement involvement, the reporting employee should ask for the Police Reporting number, and the name of the Officer that took the report. This information should be relayed when calling to report the incident in RCM.

Overview of Accident/Injury Process

After the injured worker's information has been submitted through ECOMP, the ASWC will verify the information is complete and submit them along with any forms or medical documentation, to Managed Care Advisors (MCA). MCA is a liaison office that assists employees and supervisors in the workers' compensation process for the Census Bureau. After MCA has reviewed the information, they will submit the ECOMP information and documents to the Department of Labor, Office of Workers' Compensation Program (OWCP). At this point the paperwork will be reviewed again and given a claim number. Further information on the claim may come from either MCA or OWCP. It is important that you answer any correspondence received from these offices.

If you are entitled to Continuation of Pay (COP), this authorization comes from MCA. During the COP period, if you are offered a temporary assignment that conforms to your medical restrictions, you must accept the assignment or risk losing your eligibility for COP.

Completing accident forms

One of the forms that will be required for any injury is the CA-1, *Federal Employee's Notice of Traumatic Injury and Claim for Continuation of Pay/Compensation*. You will complete the entire form in the ECOMP system.

Enter complete information on any third party (other than a respondent) who may have contributed to the accident. If you cannot provide full information on any third party (other than a respondent) who may have contributed to the accident. If you

cannot provide full information immediately, note that the information will be supplied later.

You will be able to submit any additional documents (i.e., medical bills) through ECOMP.

**Instructions for
completing the CA-1,
Federal Employee's
Notice of Traumatic
Injury and Claim for
Continuation of
Pay/Compensation**

1. From your home computer/laptop:
 - a. Access the Internet via Internet Explorer.
 - b. Go to <https://www.ecomp.dol.gov/> and press enter. (For an online tutorial, click "Filing Forms as an Injured Worker.")
 - c. If you are using the ECOMP Portal for the first time, please follow the links to "Sign In/Register" on the home page and complete the registration process. If you have already registered, click "Sign In/Register" and log on to the ECOMP Portal.
 - d. During registration, when asked to identify the part of government for which you worked at the time/date of your injury/illness, please select the following from the drop-down list:

Drop Down
List

Select (using the ▾ arrow)

Department

"Department of Commerce"

Agency-Group

"Census"

Agency

"Bureau of the Census, All Other"

Duty Station

"Regional Census Center-Location-State" corresponding to the regional office for which you work and the state in which you reside
Example: If you work out of the Philadelphia region but reside in Suitland, select "Regional Census Center-Philadelphia-MD"

- e. When prompted for your immediate supervisor's email, ***you MUST enter the ASWC's Name***. The ASWC is the supervisor of record for filing claims through ECOMP. **Do not use your immediate supervisor's email address as this will delay filing of your claim.**
- f. After completing your registration, access the confirming email sent to the email address you provided. Click on the link provided in the email to complete registration and activate your account. (The activation link expires in 24 hours; if you access after 24 hours you will have to re-register.)
- g. Sign in to the ECOMP Portal to file your claim.

Filing a Workers' Compensation Claim in ECOMP

1. Once you sign in, click on the link to “File a New Form” and follow instructions for filing CA-1 or CA-2.
2. Based on your registration, name, work location and supervisor email will be pre-populated. To successfully file the form, all other fields must be completed.

*** * * NOTICE OF TITLE 13 REQUIREMENTS * * ***

IF your injury occurred at the location of a respondent, DO NOT enter the respondent’s street address on form CA-1 or CA-2. To avoid a Title 13 violation, when completing:

<u>Form</u>	<u>Corresponding Field</u>	<u>Enter/Type into this Field</u>
CA – 1	Field #9: Address	“Title 13 Protected”

You may provide city, state, and zip code, as these fields are required.

Additional Information

If you incur expenses for an on-the-job injury, you **cannot** claim it on your D-308, *Daily Pay and Work Record* or E-308, *Electronic Daily Pay and Work Record*. These expenses will be claimed either on OWCP-915, *Claim For Medical Reimbursement* or OWCP-957, *Medical Travel Refund Request* that you will receive from the CCSI. This includes payment for prescriptions and mileage accrued going to and from doctor appointments.

Topic 5: Assaults

General

An assault of any kind is considered a violation of your civil and human rights. If you sense danger from a respondent and feel threatened to carry on your census duty, leave the scene at once. While you cannot always avoid trouble or protect yourself, there are laws to protect you in the event of an assault.

If you are ...	Then you should ...
<p>Physically injured</p> <p>or</p> <p>Struck or touched in an offensive manner</p> <p>or</p> <p>Verbally threatened or intimidated</p>	<ul style="list-style-type: none"> • Retreat to a safe place. • Immediately notify the local police and fill out a police report • Get emergency medical treatment, if necessary. Contact the Area Specialist for Workers' Compensation (ASWC) at 1-800-819-4215 AND the Administrative Specialist at the Regional Census Center (toll free 1-855-236-2020, Option #3) as soon as possible for documents to be filed for injury. • Contact your supervisor to report the incident • Report the incident to the Remedy Case Management (RCM) Incident Reporting System at (855) 236-2020, option #1. Once the incident is reported and placed in Remedy Case Management (RCM), it will be assigned for a member in the Office of Security (OSY) to investigate. The incident should be reported immediately. The purpose of the immediate time-frame is to provide details while events are fresh and can be more accurately recalled. Immediately reporting the assault may also increase the possibility of recovering property, and timely apprehension of the perpetrator. • Forward your completed forms and a copy of the police report (or provide the police report number) to the Regional Census Center.

Completing accident forms

For physical injuries, you will need to complete a CA-1, *Federal Employee's Notice of Traumatic Injury and Claim for Continuation of Pay/Compensation*. Contact the ASWC at 1-800-819-4215 for this form. Refer to Topic 4 for instructions on completing this form. Return this form to the ASWC within 48 hours.

DO NOT ENTER ANY TITLE 13-PROTECTED INFORMATION INTO ECOMP. CONTACT ASWC FOR GUIDANCE IF NEEDED.

Extended delay from returning to duty

If you are delayed from returning to duty due to injuries sustained from your accident, it is your responsibility to promptly provide medical documentation specifying in detail the nature of your disability. If alternate duties are offered to you until you are fully recovered, you are generally required to accept them. Contact the ASWC and your supervisor to discuss particulars regarding the Workers Compensation Program.

Topic 6: Accident/Injury/Property Damage Forms Chart

General

Whenever you sustain an injury or loss, or if you cause an injury or loss to someone, you must complete certain forms detailing the nature of the injury or loss. Use the chart below to determine which forms you must complete. The chart also includes the time frame in which you must submit the forms in order to comply with reporting requirements.

Figure 5-1: Preparation and Distribution Chart of Forms Required in Injury and/or Accident Cases

Type of Injury	Forms Required	Prepared By	When Prepared	Remarks
Employee Injury	CA-1, Federal Employees Notice of Traumatic Injury and Claim for Continuation of Pay/ Compensation Items 1-15	Injured Employee	Within 48 hours	Submitted electronically through ECOMP. Contact Administrative Specialist for Workers Compensation (ASWC) if you cannot submit electronically. ASWC will send you a hard copy to sign and return after being notified of your injury. Employees must notify their ASWC immediately after any work-related injury. The ASWC will email instructions for completion of the CA-1 through the electronic ECOMP system. Must be completed by the injured employee or by someone acting on his/her behalf. Must be completed to file a workers' compensation claim.
	Item 16	Witness (if applicable)	As soon as possible after injury	
	Note of responsible third party	Injured Employee	As soon as possible after injury	No title 13 information is to be entered/submitted. Send later if information isn't immediately available

Type of Injury	Forms Required	Prepared By	When Prepared	Remarks
	Items 17-38 Items a, b, and c	ASWC	As soon as possible after injury	
	OSHA 301	Injured employee and Administrative Specialist in RCC	Within 48 hours	<p>Submitted electronically through ECOMP. Contact ASWC, supervisor and Admin Specialist for safety ASWC will email instructions for registering and completing the OSHA 301 in ECOMP.</p> <p><i>Contact RCC Admin specialist for safety if you cannot complete the form electronically.. In the event of a hospitalization, fatality, amputation or loss of an eye</i></p> <p>RCC MUST CALL HSB IMMEDIATELY 301-763-3711. Leave a message if no answer. This is a OSHA REQUIREMENT.</p>
	CA-16, Authorization for Treatment	ASWC and Physician	As soon as possible but no later than 7 days after injury	This form will be faxed to the physician by the ASWC after being notified of the injury. Primarily used to authorize emergency medical treatment for an employee while on official duty.
	- or -			
	CA-20, Attending Physician's Report	Physician	Physician completes only if a narrative report or a CA-16 has not been completed.	This form will be provided to you by the ASWC after being notified of the injury. Physician completes only if a narrative report or a CA-16 has not been completed.

Type of Injury	Forms Required	Prepared By	When Prepared	Remarks
Motor Vehicle Accident (without bodily injury)	SF-91, Operator's Report of Motor Vehicle Accident	Operator of Vehicle	Within 48 Hours	This form is located in Appendix A of the Employee Handbook. Must be carried in each vehicle. Must be prepared in entirety. Copy must be submitted to HSB. Attach any police reports and keys or send them to RCC as soon as received. RCC must scan to HSB.
	SF-94, Statement of Witness	Witness	Within 48 Hours	This form is located in Appendix A.
	OSHA 301	Injured employee and Administrative Specialist in RCC	Within 48 Hours	Submitted electronically through ECOMP. Contact ASWC, supervisor and Admin Specialist for safety. ASWC will email instructions for registering and completing the OSHA 301 in ECOMP.
Motor Vehicle Accident (with bodily injury)	All forms for Motor Vehicle Accident without bodily injury and all Employee Injury forms			In the event of a hospitalization, fatality, amputation or loss of an eye RCC MUST CALL HSB IMMEDIATELY 301-763-3711. Leave a message, if no answer. This is a OSHA REQUIREMENT.
Claims for loss of or damage to employee's personal property	CD-224, Employee Claim for Loss of or Damage to <u>Personal Property</u> CD-137, Report of Injury, Illness Accident or Fatality (rev. 2/15)	Employee	Within 10 days after accident	This form is located in Appendix A. If the personal property must be repaired, submit a bill for the repair cost with the CD-224. (See Chapter 6, Topic 3 for details.)

Type of Injury	Forms Required	Prepared By	When Prepared	Remarks
Claims for loss or damage by third party due to possible negligence or wrongful act by Census employee	SF-95, Claim for Damage, Injury or Death	Claimant	As soon as possible but no later than 2 years after date	Form SF-95 will be sent to the claimant by the Regional Census Center.
	CD-224, Employee Claim for Loss of or Damage to <u>Personal Property</u>			
	CD-137, Report of Injury, Illness Accident or Fatality (rev. 2/15)			

Submission of forms

All CA-series should be returned to the ASWC within 48 hours of completion. All other forms should be returned to the RCC. For additional information on a claim filed, contact the ASWC. For additional information on other claims filed, contact the Administrative Specialist.

Topic 7: Liability and Accountability for all Title 13 Materials and Data

Overview

As an employee of the U.S. Census Bureau you are assigned materials to use solely to conduct Census work. All of these supplies are property of the federal government and may contain Title 13 (Census Confidential, 13 United States Code (U.S.C.), Section 9) data. It is your responsibility to safeguard these materials from being damaged, stolen or lost. Please carefully read your responsibilities below on this matter.

Protecting confidentiality of information

The Census Bureau informs respondents through a statement on all questionnaires, schedules, and public-use forms that the data they provide is required by law to be kept in strict confidence. The Bureau's reputation for nondisclosure of data is a major factor in obtaining the cooperation of respondents. After you have collected confidential survey information from your respondent(s), it is now up to you to protect it from being damaged, stolen or lost. Remember, if items are damaged, stolen or lost because of negligence then you may be liable to reimburse the government for the full cost of the materials

The criminal code of the United States provides penalties for the theft, embezzlement, conversion of, or willful damage to Government property.

Under the Federal Employee Compensation Act, the federal workers' compensation program is the sole governmental source of recompense for work related injuries and illnesses. Employees with workers' compensation claims must notify the federal Office of Workers' Compensation Programs (OWCP) of any compensation received from private insurance or third party legal action/settlement. However, there is no exception from Title 13 confidentiality requirements that permits an employee or former employee to release protected information for the purpose of making a third party claim for recovery against a respondent. Due to the confidentiality provisions of Title 13 of the United States Code, the OWCP does not require Census Bureau employees to provide third party information or to pursue a third party claim of recovery to seek or receive workers' compensation benefits. **DO NOT ENTER ANY TITLE 13-PROTECTED INFORMATION INTO ECOMP!**

Returning Materials

You must return all census materials when directed by your supervisor, or when you are leaving Census Bureau employment.

Toll Free Number for Reporting Loss/Stolen or Missing Sensitive Information

If a Census employee has discovered that sensitive document(s) (Admin records, Payroll records, official census badge, etc.) and/or electronic device(s), CD's, DVD's, which contain PII (Personal Identifiable Information) is/are Lost, Missing, or Stolen (LMS) the employee is to do the following:

- Calls the Decennial Service Center (DSC) at 855-236-2020, option #1, within 1 hour of discovery of the LMS document(s) or electronic device(s) to report the incident and obtain a ticket number.
- Contacts their Supervisor and/or the Area Census Office (ACO) Point of Contact (POC) to provide information on the incident including the ticket number provided by the DSC.

When calling to report an incident to the DSC, the following information will be requested:

- Your name
- ACO/RCC name and/or number
- Date, time and location of incident.
- Summary of incident detailing what is lost, missing or stolen.
- Was the data encrypted?
- Was it password protected?
- Was there any PII or Title 13 breached by the lost, missing, or stolen equipment or other sensitive documents?

If the police were contacted prior to placing the call to DSC, FLD staff employee should provide the police report number, name of the officer that took report, time the report was taken, and which police department the report was made.

Additionally, once the initial call is placed into DSC, all further updates to the tickets have to be made by the POCs at the RCC or HQ. DSC call handlers cannot open the ticket for updates after the initial call is completed.

What will the Decennial Service Center do after your call

Once the DSC has been notified of LMS documents and /or electronic equipment is LMS, a ticket is generated by Remedy Case Management (RCM). The POC at the DSC will provide the caller with the ticket number. Once the report has been generated by DSC an automated notification is sent to the HQ FLD Division POC and RCC/ACO POC as well as other areas in Census such as the Office of Security (OSY).

What to do after calling the Decennial Service Center

- If you have not already called your police department, please call them and fill out a report and obtain a report number, the name of the officer that took report and a copy of the police report when available. Provide a copy of the police report when it becomes available to your Supervisor and/or ACO POC. The ACO POC needs to contact RCC POC so they can update BC Remedy.
- Call your supervisor immediately and report the incident. Provide your supervisor with the Remedy ticket number and police report number (if available). You and your supervisor should make arrangements for replacing the lost, missing, or stolen item(s) as soon as possible.
- Your supervisor who received the notification will report details (including the police report number) up the chain of command, until all parties in the chain are informed.

What will RCM do after your call?

RCM will create a ticket number and send an electronic notification to the groups needing to take action such as FLD Division POC, RCC POC, the Office of Security (OSY), the Privacy Office, and others as needed.

Chapter 6: Personal Property and Damage Claims

Topic 1: Claim Information

General

While conducting census activities is often a rewarding and pleasant undertaking, it can sometimes be stressful. On rare occasions, you might encounter a ferocious dog or, you might suffer damage to a valuable personal item. Whatever the circumstance, you might be eligible to receive reimbursement for losses or damages to personal property.

Legal representation

If court action is brought against you (or your estate) as a result of an accident or other legal proceeding while on official census duty, the Attorney General will defend you in court.

Within three business days, you or your representative must deliver to your Area Census Office Manager (ACOM) (through your immediate supervisor) all processes and pleadings served on you. In addition, if you receive any processes, proceedings, or advance information regarding the start of a civil suit, immediately advise your ACOM by telephone, fax, or visit to the office.

Federal Tort Claims Act

The Federal Tort Claims Act (FTCA) covers employees for liability incurred while using their vehicles on official business. State law governs when an employee is deemed to be “on official business,” so FTCA coverage can vary from state to state.

The Bureau of the Census recommends that employees who use their vehicle for official business comply with all applicable state laws, and carry sufficient insurance to protect themselves in case FTCA coverage is unavailable.

Physical damage insurance

Any damage to your vehicle or other major personal property must be covered by your own physical damage insurance. The insurance is intended to cover expenses resulting from collisions, vandalism, and thefts. Except in very rare circumstances, the Bureau of the Census will not reimburse you for damage to your vehicle.

Topic 2: Permissible Claims

Claim conditions

There are five conditions you must meet to receive reimbursement for loss of, or damage to, your personal property:

- The loss of or damage to your personal property must have resulted from your official census duty
- You file a claim within two years after the incident occurs
- The loss or damage was not caused wholly or partly by your negligent or wrongful act
- Witnesses can verify the loss or damage, or you have other evidence such as a receipt or similar document which proves the value of the property
- It was reasonable for you to have the property on your person at the time of the loss or damage

Special claim consideration

The Bureau of the Census will consider claims for loss of or damage to personal property in unusual circumstances if a serious inequity would otherwise occur.

Definition: ‘personal property’

The term ‘personal property’ includes the garments, handbags, shoes, and other items that you wear while conducting Census Bureau business. It may also include your bicycle or other mode of transportation that does not require gas, an electric motor, or vehicle insurance. “Personal property” does not include motorized vehicles for which insurance is required.

Type of events

Certain events can result in a loss of or damage to your personal property. If such an event occurs while on official duty, you may file a claim for reimbursement for any damage or loss.

- Forced evacuation from airports, train or bus stations, or other transportation buildings which result in loss of luggage, damage to clothing, etc., when traveling on official census business
- Exposure to extraordinary risks
- Unpredictable behavior of animals
- Damage or loss of property specifically used for the benefit of the federal government at the direction or

approval of your supervisor

- Theft of personal property (used for official business) for which you can establish its prior existence and ensure that reasonable measures were taken for its security

Items not reimbursed

In certain circumstances, damage or loss of personal property cannot be reimbursed by the Bureau of the Census:

- Theft of items whose prior existence cannot be proven
- Theft of articles of excessive value, or those that can easily be stolen
- Loss of currency or intangible property unless payable under other conditions
- Loss or damage to your vehicle
- Loss or damage that is covered by insurance
- Loss or damage to tattered or unserviceable property
- Loss or damage to property that is owned by the U.S. and for which you are not financially responsible
- Loss or damage to property that you normally use for your own private business or profit
- Repair estimate fees for damaged property which your ACOM has not approved in advance of your obtaining the estimate
- Property that is acquired, possessed, or transported in violation of the law

Topic 3: Making A Personal Property Claim

How to make a personal property claim

Complete a CD-224, *Employee Claim for Loss of or Damage to Personal Property*, for each qualified occurrence. Other forms may be required for you to complete depending on the nature of the incident.

In cases where an injury also occurred, contact the Administrative Specialist at the Regional Census Center toll free (1-855-236-2020, Option #3) for the appropriate forms to file a workers' compensation claim.

Providing evidence

Provide all appropriate supporting documentation as evidence to support your claim. If you cannot provide the proper evidence, prepare a statement indicating why supporting documentation is unavailable or is impractical to obtain.

List of supporting documentation

These items are considered appropriate supporting documentation:

- A statement from one or more witnesses which gives details of the incident
- A statement that the property has been recovered or replaced in kind
- A detailed written estimate of the repair cost that is prepared by a person or company licensed to make such repairs (*If a fee is charged for the estimate, **first** obtain your ACOMs or Area Manager approval for guarantee of fee reimbursement.*)
- Itemized repair bill and/or receipt for repairing damaged property
- Receipts or similar documents proving the value or cost of the original property
- A statement of insurance coverage, including copies of claim papers if you made a claim through your insurance company

**Submission of the
CD-224, *Employee
Claim For
Loss/Damage to
Personal Property*, and
other required forms**

Attach the completed CD-224 (and other required forms) and any supporting documentation to your payroll form and give to your supervisor for submission to the ACO (Area Census Office).

Replacement cost

If your claim is approved, you will receive an amount equal to the estimated fair market value of the property at the time and place of your loss.

**Repair cost versus
replacement cost**

If the cost of repairing the property is less than the replacement cost of the property, you will receive an amount equal to the repair cost.

This Page Intentionally Left Blank

Chapter 7: Employee Relations

Topic 1: Equal Employment Opportunity (EEO)

General

The following federal laws govern the EEO program throughout the federal government.

- *Title VII of the Civil Rights Act of 1964*, as amended. Protects all employees and applicants from employment discrimination based on race, color, gender, religion, sexual orientation and or gender identity and national origin.
- *Age Discrimination in Employment Act of 1967*, as amended. Protects employees and applicants who are 40 years or older from employment discrimination based on age.
- *Rehabilitation Act of 1973*. Protects qualified individuals with disabilities from employment discrimination based on disability.
- *Equal Pay Act*. Protects employees from discrimination on the basis of sex in pay for equal work on jobs requiring equal skill, effort and responsibility.
- *The Genetic Information Nondiscrimination Act of 2008 (GINA)*. Protects employees and applicants from employment discrimination based on genetic information.
- *The Pregnancy Discrimination Act*. Protects against illegal discrimination against a woman because of pregnancy, childbirth, or a medical condition related to pregnancy or childbirth.

Note: In addition, regulations of the Equal Employment Opportunity Commission (EEOC) forbid restraint, interference, coercion, discrimination or reprisal at any stage in the processing of an employment complaint under the laws above, including the counseling stage.

All employees should be made aware of the Census Bureau's EEO policy at the time of training. Applicants should be advised by display of EEO posters in the ACO and at recruiting/testing sites.

**The Census Bureau's
Policy on EEO**

The Census Bureau is committed to provide equal opportunity in employment for all persons without regard to race, color, religion, gender, sexual orientation, national origin, age, GINA or disability.

Managers, supervisors and employees alike have responsibilities to ensure that the Census Bureau's actions foster an environment of equal opportunity in the work place. Policies, practices, procedures, and actions must be free of unlawful discrimination.

This includes all aspects of personnel management and their effects upon the hiring, placement, training, advancement, recognition, and retention of qualified individuals. Sexual harassment also is prohibited and steps will be taken to eliminate it when it exists. Employees have the right to seek redress for alleged discrimination and they are protected from reprisal in exercising this right.

Employees or applicants for employment with the Census Bureau who believe that they have been discriminated or retaliated against, must contact an EEO Office or an EEO Counselor within 45 calendar days of the alleged discrimination. For more information, contact:

U.S. Census Bureau
EEO Office
4600 Silver Road
Washington, DC 20233
(301) 763-2853, then select 1 for EEO Program Assistance
(800) 872-6096, then select 1 for EEO Program Assistance
Fax (301) 763-4460

Topic 2: Sexual Harassment

Census Bureau Policy Statement

The Census Bureau will not tolerate sexual harassment. Training is conducted that informs supervisors and managers about sexual harassment and how it can be prevented in the work place. The following is the Census Bureau's Policy Statement on Sexual Harassment:

Recognizing that there are many forms of sexual harassment, the Census Bureau, in accordance with case law, will not tolerate nor condone the following: (1) unwelcome verbal suggestive remarks, sexual insults, innuendoes, jokes, and humor about sex or gender-specific traits, sexual propositions, and threats; (2) unwelcome nonverbal suggestive or insulting sounds, leering/ogling, whistling, gestures of a sexual nature, and sexually graphic materials; and (3) unwanted physical contact, including but not limited to, cornering, touching, pinching, brushing the body, and actual or attempted rape or assault. Neither the Agency's e-mail system nor computer equipment should be used to transmit or download material of a sexually graphic nature. The Census Bureau policy on sexual harassment applies to all employees and covers harassment between supervisors and subordinates, between employees, by employees outside the workplace while conducting government business, and by non-employees while conducting business in the Census Bureau's workplace.

Available Relief

Victims of sexual harassment have several means of redress, including:

- Seeking help from their supervisor or higher level official.
- Initiating a discrimination complaint by contacting an EEO Counselor or the Department of Commerce/Office of Civil Rights (DOC/OCR) within 45 days of the harassment.
- Reporting the incident to the DOC Office of the Inspector General (OIG).
- Reporting the incident as a prohibited personnel practice to the Office of Special Counsel.
- Reporting the incident to the Employees Relations Office within HRD at Census HQ.

Topic 3: Fraud, Waste, and Abuse

Recognizing fraud, waste, and abuse

Fraud, waste, and abuse of federal government funds and property occur through—

- violations of the Federal law or regulations,
- mismanagement,
- theft,
- abuse of authority, or
- conditions leading to substantial danger to health and safety.

Reporting acts of fraud, waste, and abuse

Each employee has an obligation to report to his/her supervisor, or to the Office of Inspector General (OIG), information concerning the possible existence of a violation of law, rules, or regulations; mismanagement; gross waste of funds; abuse of authority; or a substantial and specific danger to public health or safety. Employees are protected by law from reprisal for making any disclosure supported by reasonable evidence.

Make reports directly to the Department of Commerce, Office of the Inspector General via the following means:

- **Telephone** - The OIG Hotline is staffed 24 hours a day, 7 days a week.

Toll Free (800)-424-5197

In the DC metro area (202)-482-2495

TTD Toll Free (855)-860-6950

TTD in the DC metro area (202)-482-5923

Fax (855)-569-9235

- **Mail**

Office of Inspector General

Complaint Intake Unit, Mail Stop 7886

1401 Constitution Avenue, N.W.

Washington, DC 20230

Confidentiality

All information you report will be kept confidential. You may remain anonymous if you desire. However, if you do give your name, it will not be disclosed without your prior consent unless absolutely necessary for judicial or administrative proceedings.

Topic 4: Pursuing Complaints

Pursing complaints of discrimination

If you believe you have been discriminated against on any of the above, you may pursue a complaint through the Census Bureau's EEO complaint process. You must contact the EEO office within 45 calendar days from the date of the matter you allege is discriminatory or, in the case of personnel action, within 45 calendar days from the effective date of the action.

The EEO office may be contacted at—

(800) 872-6096, then select 1 or

(301) 763-2853, then select 1 or

Fax (301) 763-4460

Topic 5: ACO Administrative Grievance Procedure

ACO Administrative Grievance Procedure

As an Area Census Office (ACO) employee, you have the right to file a grievance concerning your employment under the ACO Administrative Grievance Procedure. Should you experience concern or dissatisfaction with some aspect of your employment, you should first attempt to resolve the matter by talking with your supervisor. If this does not resolve the problem, you may file a grievance.

You may consult with management regarding any questions or issues you have dealing with the ACO Administrative Grievance Procedure. The *ACO Administrative Grievance Intake Form*, D-244, is available in Appendix A of this handbook for your use.

You are considered to have elected the 2020 Census Administrative Grievance forum at the time you complete, in writing, the D-244, *ACO Administrative Grievance Intake Form*, and present it to your supervisor. If you have already filed an EEO complaint about the same issue, the grievance will be dismissed.

Note: If you separate from the Census Bureau (i.e., Terminate for Lack of Work) you are not entitled to file a complaint using the Administrative Grievance Procedure.

Basic points when filing a grievance

- You must file a grievance with the appropriate ACO manager who supervises your work unit (i.e., Administrative Manager, Census Field Manager, Recruitment Manager, or Information Technology Manager).
- You must present the grievance in writing on the D-244 within 15 calendar days of the date of the act or occurrence or the date you become aware of the grievable issue. You must complete items 1-7 on the D-244.
- You will have a reasonable amount of official work time to present the grievance. However, you are not entitled to use official work time or the Census Bureau's equipment to prepare the grievance.
- You will receive a final written decision on the D-244 within 15 calendar days after submitting the grievance to the appropriate management official.

Nongrievable matters

Certain matters are not grievable. Please refer to the following items to determine whether your matter is grievable under the ACO Administrative Grievance Procedure—

- a decision which is appealable to the Merit Systems Protection Board or is subject to final administrative review by the Office of Personnel Management or the Equal Employment Opportunity Commission
- published policy or regulations of Field Division, The Census Bureau, or the Department of Commerce
- non-selection for a promotion or the failure to receive a noncompetitive promotion
- the granting of or failure to grant an employee award, or the adoption of or failure to adopt an employee suggestion or invention
- the receipt of or failure to receive an award or quality step increase
- a preliminary warning notice of an action which, if effected, would be covered under the grievance system or excluded from coverage under the first item of this list
- the substance of the critical elements and performance indicators of an employee's position
- any separation action
- a matter previously grieved by the same employee
- an action taken in response to a formal agreement that was voluntarily entered into by the employee which assigns that employee from one geographical location to another

Topic 6: Important Contact Information

General

This topic provides a list of phone numbers and Web sites for you. Enter your Area Census Office telephone number and your immediate supervisor's phone number, both of which will be provided to you on your first day of training. Keep this list updated and in an easily accessible place for your reference.

Phone Numbers:

My Area Census Office _____

My supervisor _____

Emergency (Police, Fire, and Ambulance) 911

Payroll and Personnel Hotline 1 (855) 236-2020, Option #3

Decennial Service Center 1 (855) 236-2020

EEO Assistance Program 1 (800) 872-6096, select 1

Fraud, Waste, and Abuse Hotline. 1 (800) 424-5197

Office of Special Counsel (OSC)..... 1 (800) 872-9855

Web sites:

Census Bureau No Fear Act Policy www.census.gov/eeo/

Discrimination Laws..... www.census.gov/eeo/

EEO Complaint Process..... www.eeoc.gov

Whistleblower Acts and Protection Information www.osc.gov

This Page Intentionally Left Blank

Appendix A: Forms for Employee Use

Available forms

This appendix contains a set of perforated forms that can be detached for your use. If you need more than one form, make copies at your local copy center and claim reimbursement for those copies on your Form D-308 or E-308. Attach receipts or send photo of receipt for copy jobs costing \$5 or more. This appendix includes the following items:

Forms
CD-224, Employee Claim for Loss or Damage to Personal Property
D-149, Correction Request
D-244, ACO Administrative Grievance Intake Form
SF-91, Motor Vehicle Accident Report
SF-94, Statement of Witness
SF-1152, Designation of Beneficiary
D-1199, Payment Authorization
W-4, Employee's Withholding Allowance Certificate
D-952, Most Frequently Asked Questions By Employees
D-1129, Personal Telephone Reimbursement Policy Agreement
D-198, What You Must Do To Get Your Pay Check On Time

This page intentionally left blank

EMPLOYEE CLAIM FOR LOSS OF OR DAMAGE TO PERSONAL PROPERTY
(P.L. 88-558)

INSTRUCTIONS: Submit in duplicate to Operating Unit Claims Officer. Please type.

NAME OF EMPLOYEE	OPERATING UNIT OR DEPARTMENTAL OFFICE	
NAME AND ADDRESS OF CLAIMANT. <i>If claimant is other than employee, submit names and addresses of all parties in interest. (See DAO 203-22 Section 6)</i>	CITY	AREA CODE AND PHONE NUMBER
	LOCATION OF LOSS OR DAMAGE	
	DATE OF LOSS OR DAMAGE	TOTAL AMOUNT OF CLAIM

DESCRIPTION OF PROPERTY

ITEMIZED LISTING	DATE ACQUIRED	PURCHASE PRICE OR VALUE	VALUE WHEN LOST OR DAMAGED	ESTIMATED REPAIR COST

CLAIM IS FOR ☐ LOSS ☐ DAMAGE (Check One) GIVE BRIEF STATEMENT OF CIRCUMSTANCES:

CLAIM IS FOR <input type="checkbox"/> LOSS <input type="checkbox"/> DAMAGE (<i>Check One</i>) GIVE BRIEF STATEMENT OF CIRCUMSTANCES:	
WAS PROPERTY INSURED?	IF ANSWER IS "YES" GIVE NAME OF INSURER, AMOUNT OF INSURANCE CARRIED, AND RESULTS OF EFFORTS TO COLLECT IT.
<input type="checkbox"/> YES	
<input type="checkbox"/> NO	

CRIMINAL PENALTY FOR PRESENTING A FRAUDULENT CLAIM OR MAKING FALSE STATEMENTS: Fine of not more than \$10,000 or imprisonment for not more than 5 years or both. (See 62 Stat. 698, 749; 18 U.S.C. 287,1001)

CIVIL PENALTY FOR PRESENTING A FRAUDULENT CLAIM: The claimant shall forfeit and pay to the United States the sum of \$2,000, plus double the amount of damages sustained by the United States. (See R.S. Sec. 3490, 5438; 31 U.S.C. 231)

ADMINISTRATIVE PENALTY: Removal from the service.

I make this claim with full knowledge of the penalties for making a false claim, and certify that I am entitled to any payments.

SIGNATURE OF CLAIMANT	IF CLAIMANT IS NOT OWNER, STATE RELATIONSHIP	DATE

This page intentionally left blank

This page intentionally left blank



ACO ADMINISTRATIVE GRIEVANCE INTAKE FORM 2020 Census

U.S. DEPARTMENT OF COMMERCE
Economics and Statistics Administration
U.S. CENSUS BUREAU

TO BE COMPLETED BY GRIEVANT (Items 1-7)

1. TO

Deciding Official (*First, Middle Initial, Last*)

2. FROM

Grievant (*First, Middle Initial, Last*)

3. Subject of Grievance:

4. Date of Incident(s) or Date Grievant Became Aware of Issues Cited Under Section 3:

5. Date of Submission of Grievance Intake Form:

		Month			Day		
				Year			

6. Relief Requested:

7. Grievant's Signature _____

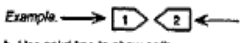




By signing this form, I certify that the information is true to the best of my knowledge and that I have not filed a complaint on the same issues under another system (e.g., EEO).

[illegible]

MOTOR VEHICLE ACCIDENT REPORT	Please read the Privacy Act State- ment on Page 3	INSTRUCTIONS: Sections I thru IX are filled out by the vehicle operator. Section X, items 72 thru 82c are filled on by the operator's supervisor. Section XI thru XIII are filled out by an accident investigator for bodily injury, fatality, and/or damage exceeding \$500.			
SECTION I - FEDERAL VEHICLE DATA					
1. DRIVER'S NAME (Last, first, middle)			2. DRIVER'S LICENSE NO./STATE/LIMITATIONS		DATE OF ACCIDENT
4a. DEPARTMENT/FEDERAL AGENCY PERMANENT OFFICE ADDRESS				4b. WORK TELEPHONE NUMBER ()	
5. TAG OR IDENTIFICATION NUMBER	6. EST. REPAIR COST \$	7. YEAR OF VEHICLE	8. MAKE	9. MODEL	10. SEAT BELTS USED <input type="checkbox"/> YES <input type="checkbox"/> NO
11. DESCRIBE VEHICLE DAMAGE					
SECTION II - OTHER VEHICLE DATA (Use Section VIII if additional space is needed)					
12. DRIVER'S NAME (Last, first, middle)		13. SOCIAL SECURITY NO./ TAX IDENTIFICATION NO.		14. DRIVER'S LICENSE NO./STATE/LIMITATIONS	
15a. DRIVER'S WORK ADDRESS				15b. WORK TELEPHONE NUMBER ()	
16a. DRIVER'S HOME ADDRESS				16b. HOME TELEPHONE NUMBER ()	
17. DESCRIPTION OF VEHICLE DAMAGE				18. ESTIMATED REPAIR COST \$	
19. YEAR OF VEHICLE	20. MAKE OF VEHICLE	21. MODEL OF VEHICLE		22. TAG NUMBER AND STATE	
23a. DRIVER'S INSURANCE COMPANY NAME AND ADDRESS				23b. POLICY NUMBER	
				23c. TELEPHONE NUMBER ()	
24. VEHICLE IS <input type="checkbox"/> CO-OWNED <input type="checkbox"/> RENTAL <input type="checkbox"/> LEASED <input type="checkbox"/> PRIVATELY OWNED		25a. OWNER'S NAME(S) (Last, first, middle)		25b. TELEPHONE NUMBER ()	
26. OWNER'S ADDRESS(ES)					
SECTION III - KILLED OR INJURED (Use Section VIII if additional space is needed)					
27. NAME (Last, first, middle)			28. SEX	29. DATE OF BIRTH	
30. ADDRESS					
A	31. MARK "X" IN TWO APPROPRIATE BOXES <input type="checkbox"/> KILLED <input type="checkbox"/> DRIVER <input type="checkbox"/> PASSENGER <input type="checkbox"/> INJURED <input type="checkbox"/> HELPER <input type="checkbox"/> PEDESTRIAN		32. IN WHICH VEHICLE FED <input type="checkbox"/> OTHER (2) <input type="checkbox"/>	33. LOCATION IN VEHICLE	34. FIRST AID GIVEN BY
	35. TRANSPORTED BY		36. TRANSPORTED TO		
37. NAME (Last, first, middle)			38. SEX	39. DATE OF BIRTH	
40. ADDRESS					
B	41. MARK "X" IN TWO APPROPRIATE BOXES <input type="checkbox"/> KILLED <input type="checkbox"/> DRIVER <input type="checkbox"/> PASSENGER <input type="checkbox"/> INJURED <input type="checkbox"/> HELPER <input type="checkbox"/> PEDESTRIAN		42. IN WHICH VEHICLE FED <input type="checkbox"/> OTHER (2) <input type="checkbox"/>	43. LOCATION IN VEHICLE	44. FIRST AID GIVEN BY
	45. TRANSPORTED BY		46. TRANSPORTED TO		
47. Pedes- trian	a. NAME OF STREET OR HIGHWAY		b. DIRECTION OF PEDESTRIAN (SW corner to NE corner, etc.) FROM TO		
	c. DESCRIBE WHAT PEDESTRIAN WAS DOING AT TIME OF ACCIDENT (Crossing intersection with signal, against signal, diagonally; in roadway playing, walking, hitchhiking, etc.)				

NSN 7540-00-634-4041
Previous edition not usable

STANDARD FORM 91 (REV. 2/2004)
Prescribed by GSA-FMR 102-34.295

SECTION IV - ACCIDENT TIME AND LOCATION <i>(Use Section VIII if additional space is needed.)</i>																													
48. DATE OF ACCIDENT	49. PLACE OF ACCIDENT (Street address, city, state, ZIP Code; Nearest landmark; Distance nearest intersection; Kind of locality (industrial, business, residential, open country, etc.); Road description).																												
50. TIME OF ACCIDENT	<div style="display: flex; align-items: center;"> <div style="width: 40px; text-align: center;">AM</div> <div style="width: 40px; text-align: center;">PM</div> </div>																												
51. INDICATE ON THIS DIAGRAM HOW THE ACCIDENT HAPPENED		52. POINT OF IMPACT <i>(Check one for each vehicle)</i>																											
<p>Use one of these outlines to sketch the scene. Write in street or highway names or numbers.</p> <p>a. Number Federal vehicle as 1, other vehicle as 2, additional vehicle as 3 and show direction of travel with arrow.</p> <p>Example: </p> <p>b. Use solid line to show path before accident and broken line after the accident. </p> <p>c. Show pedestrian by </p> <p>d. Show railroad by ++++++ </p> <p>e. Place arrow in this circle to indicate NORTH </p>		<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;">FED</th> <th style="width: 10%;">2</th> <th style="width: 80%;">AREA</th> </tr> </thead> <tbody> <tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>a. Front</td></tr> <tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>b. R. Front</td></tr> <tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>c. L. Front</td></tr> <tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>d. Rear</td></tr> <tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>e. R. Rear</td></tr> <tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>f. L. Rear</td></tr> <tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>g. R. Side</td></tr> <tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>h. L. Side</td></tr> </tbody> </table>	FED	2	AREA	<input type="checkbox"/>	<input type="checkbox"/>	a. Front	<input type="checkbox"/>	<input type="checkbox"/>	b. R. Front	<input type="checkbox"/>	<input type="checkbox"/>	c. L. Front	<input type="checkbox"/>	<input type="checkbox"/>	d. Rear	<input type="checkbox"/>	<input type="checkbox"/>	e. R. Rear	<input type="checkbox"/>	<input type="checkbox"/>	f. L. Rear	<input type="checkbox"/>	<input type="checkbox"/>	g. R. Side	<input type="checkbox"/>	<input type="checkbox"/>	h. L. Side
FED	2	AREA																											
<input type="checkbox"/>	<input type="checkbox"/>	a. Front																											
<input type="checkbox"/>	<input type="checkbox"/>	b. R. Front																											
<input type="checkbox"/>	<input type="checkbox"/>	c. L. Front																											
<input type="checkbox"/>	<input type="checkbox"/>	d. Rear																											
<input type="checkbox"/>	<input type="checkbox"/>	e. R. Rear																											
<input type="checkbox"/>	<input type="checkbox"/>	f. L. Rear																											
<input type="checkbox"/>	<input type="checkbox"/>	g. R. Side																											
<input type="checkbox"/>	<input type="checkbox"/>	h. L. Side																											
53. DESCRIBE WHAT HAPPENED (Refer to vehicles as "Fed", "2", "3", etc. Please include information on posted speed limit, approximate speed of the vehicles, road conditions, weather conditions, driver visibility, condition of accident vehicles, traffic controls (warning light, stop signal, etc.), condition of light (daylight, dusk, night, dawn, artificial light, etc.), and driver actions (making U-turn, passing, stopped in traffic, etc.).																													

SECTION V - WITNESS/PASSENGER <i>(Witness must fill out SF 94, Statement of Witness) (Continue in Section VIII.)</i>		
54. NAME (Last, first, middle)	55. WORK TELEPHONE NUMBER ()	56. HOME TELEPHONE NUMBER ()
A	57. WORK ADDRESS	58. HOME ADDRESS
B	59. NAME (Last, first, middle)	60. WORK TELEPHONE NUMBER ()
	61. HOME TELEPHONE NUMBER ()	62. WORK ADDRESS
	63. HOME ADDRESS	
SECTION VI - PROPERTY DAMAGE <i>(Use Section VIII if additional space is needed.)</i>		
64a. NAME OF OWNER (Last, first, middle)	64b. WORK TELEPHONE NUMBER ()	64c. HOME TELEPHONE NUMBER ()
64d. WORK ADDRESS	64e. HOME ADDRESS	
65a. NAME OF INSURANCE COMPANY	65b. TELEPHONE NUMBER ()	65c. POLICY NUMBER
66. ITEM DAMAGED	67. LOCATION OF DAMAGED ITEM	68. ESTIMATED COST
SECTION VII - POLICE INFORMATION		
69a. NAME OF POLICE OFFICER	69b. BADGE NUMBER	69c. TELEPHONE NUMBER ()
70. PRECINCT OR HEADQUARTERS	71a. PERSON CHARGED WITH ACCIDENT	71b. VIOLATION(S)

SECTION VIII - EXTRA DETAILS

SPACE FOR DETAILED ANSWERS. INDICATE SECTION AND ITEM NUMBER FOR EACH ANSWER. IF MORE SPACE IS NEEDED, CONTINUE ITEMS ON PLAIN BOND PAPER.

PRIVACY ACT STATEMENT

The information on this form is subject to the Privacy Act of 1974 (5 U.S.C. section 552a). Authority to collect the information is Title 40 U.S.C. Section 491 and title 31 U.S.C. Section 7701. The information is required by Federal Government agencies to administer motor vehicle programs, including maintaining records on accidents involving privately owned and Federal fleet vehicles, and collecting accident claims resulting from accidents. Federal employees, and employees under contract, will use the information only in the performance of their official duties. Routine uses of the collected information may include disclosures to: appropriate Federal, State, or local agencies or contractors when relevant to civil, criminal, or regulatory investigations or prosecutions; the Office of Personnel Management and the General Accounting Office for program evaluation purposes; a Member of Congress or staff in response to a request for assistance by the individual of record; another Federal agency, including the Departments of Treasury and Justice, or a court under judicial proceedings; agency Inspectors General in conducting audits; private insurance and collection agencies (including agencies under contract to Treasury to collect debt), and to other agency finance offices for fiscal management and debt collection. Furnishing the requested information is mandatory, including the Social Security Number or Taxpayer's Identification Number (TIN) for use as a unique identifier to ensure accurate identification of individuals or firms in the system.

SECTION IX - FEDERAL DRIVER CERTIFICATION

I certify that the information on this form (Sections I thru VIII) is correct to the best of my knowledge and belief.

72a. NAME AND TITLE OF DRIVER

72b. DRIVER'S SIGNATURE AND DATE

SECTION X - DETAILS OF TRIP DURING WHICH ACCIDENT OCCURRED

73. ORIGIN

74. DESTINATION

75. EXACT PURPOSE OF TRIP

76. TRIP BEGAN	DATE	TIME (Include AM or PM)	77. ACCIDENT OCCURRED	DATE	TIME (Include AM or PM)
78. AUTHORITY FOR THE TRIP WAS GIVEN TO THE OPERATOR <input type="checkbox"/> ORALLY <input type="checkbox"/> IN WRITING (Explain)			79. WAS THERE ANY DEVIATION FROM DIRECT ROUTE? <input type="checkbox"/> NO <input type="checkbox"/> YES (Explain)		
80. WAS THE TRIP MADE WITHIN ESTABLISHED WORKING HOURS? <input type="checkbox"/> YES <input type="checkbox"/> NO (Explain)			81. DID THE OPERATOR, WHILE ENROUTE, ENGAGE IN ANY ACTIVITY OTHER THAN THAT FOR WHICH THE TRIP WAS AUTHORIZED? <input type="checkbox"/> NO <input type="checkbox"/> YES (Explain)		
82. COMPLETED BY DRIVER'S SUPERVISOR	a. DID THIS ACCIDENT OCCUR WITHIN THE EMPLOYEE'S SCOPE OF DUTY				
	b. COMMENTS				
83a. NAME AND TITLE OF SUPERVISOR			83b. SUPERVISOR'S SIGNATURE AND DATE		83c. TELEPHONE NUMBER
					()

STANDARD FORM 91 (REV. 2/2004) PAGE 3

SECTION XI - ACCIDENT INVESTIGATION DATA

84. DID THE INVESTIGATION DISCLOSE CONFLICTING INFORMATION. ☐ NO ☐ YES (If checked, explain below.)

85. PERSONS INTERVIEWED

NAME		DATE	NAME		DATE
a.			c.		
b.			d.		

86. ADDITIONAL COMMENTS (Indicate section and item number of each comment).

SECTION XII - ATTACHMENTS

87. LIST ALL ATTACHMENTS TO THIS REPORT

SECTION XIII - COMMENTS/APPROVALS

88. REVIEWING OFFICIAL'S COMMENTS

89. ACCIDENT INVESTIGATOR

a. SIGNATURE	b. DATE
--------------	---------

c. NAME (First, middle, last)

d. TITLE

e. OFFICE

f. OFFICE TELEPHONE NUMBER

AREA CODE	NUMBER	EXTENSION
-----------	--------	-----------

90. ACCIDENT REVIEWING OFFICIAL

a. SIGNATURE	b. DATE
--------------	---------

c. NAME (First, middle, last)

d. TITLE

e. OFFICE

OFFICE TELEPHONE NUMBER

AREA CODE	NUMBER	EXTENSION
-----------	--------	-----------

STANDARD FORM 91 (REV. 2/2004) PAGE 4

STATEMENT OF WITNESS*(Attach additional sheets if necessary)*

1. DID YOU SEE THE ACCIDENT?

2. WHEN DID THE ACCIDENT HAPPEN?

a. TIME

a.m.

b. DATE

p.m.

FORM APPROVED

O.M.B. NUMBER

3090-0118

3. WHERE DID THE ACCIDENT HAPPEN? *(Give street location and city)*

4. TELL IN YOUR OWN WAY HOW THE ACCIDENT HAPPENED

5. WHERE WERE YOU WHEN THE ACCIDENT OCCURRED?

6. WAS ANYONE INJURED, AND IF SO, EXTENT OF INJURY IF KNOWN?

7. DESCRIBE THE APPARENT DAMAGE TO PRIVATE PROPERTY

8. DESCRIBE THE APPARENT DAMAGE TO GOVERNMENT PROPERTY

9. IF TRAFFIC CASE,
GIVE APPROXIMATE
SPEED OF:a. GOVERNMENT VEHICLE
Miles
per Hr.b. OTHER VEHICLE
Miles
per Hr.10. GIVE THE NAMES AND ADDRESSES OF ANY OTHER WITNESSES TO THE ACCIDENT *(If known)*

a. NAMES

b. ADDRESSES *(Include ZIP Code)*WITNESS
COM-
PLETING
THIS
FORM11. HOME ADDRESS *(Include ZIP Code)*

12. WITNESS (Print Name)

a. HOME TELEPHONE NO.

Sign
here

b. TODAY'S DATE

13. BUSINESS ADDRESS *(Include ZIP Code)*

TELEPHONE NO.

14. INDICATE ON THE DIAGRAM BELOW WHAT HAPPENED:

1. Number Federal vehicle as 1—other vehicle as 2—additional vehicle as 3, and show direction of travel by arrow

(Example: → 1 2 ←)

2. Use solid line to show path before accident

Broken line after accident

3. Show pedestrian by → ○

4. Show railroad by ++++++

5. Give names or numbers of streets or highways

6. Indicate north by arrow in this circle

FILE REFERENCE:

This office has been notified that you witnessed an accident which occurred

It will be helpful if you will answer, as fully as possible, the questions on the other side of this letter. Please read the Privacy Act Statement below.

Your courtesy in complying with this request will be appreciated. An addressed envelope, which requires no postage, is enclosed for your convenience in replying.

Sincerely

Enclosure

Use by the public is voluntary. In compliance with the Privacy Act of 1974, the following information is provided: Solicitation of the information requested on this form is authorized by Title 40 U.S.C. Section 491. Disclosure of the information by a Federal employee is mandatory as it is the first step in the Government's investigation of a motor vehicle accident. The principal purposes for which the information is intended to be used are to provide necessary data for use by legal counsel in legal actions resulting from the accident, and to provide accident information/statistics for use in analyzing accident causes and developing methods of reducing accidents. Routine use of the information may be by Federal, State or local governments or agencies, when relevant to civil, criminal, or regulatory investigations or prosecution.

FILE REFERENCE:

This office has been notified that you witnessed an accident which occurred

It will be helpful if you will answer, as fully as possible, the questions on the other side of this letter. Please read the Privacy Act Statement below.

Your courtesy in complying with this request will be appreciated. An addressed envelope, which requires no postage, is enclosed for your convenience in replying.

Sincerely

Enclosure

Use by the public is voluntary. In compliance with the Privacy Act of 1974, the following information is provided: Solicitation of the information requested on this form is authorized by Title 40 U.S.C. Section 491. Disclosure of the information by a Federal employee is mandatory as it is the first step in the Government's investigation of a motor vehicle accident. The principal purposes for which the information is intended to be used are to provide necessary data for use by legal counsel in legal actions resulting from the accident, and to provide accident information/statistics for use in analyzing accident causes and developing methods of reducing accidents. Routine use of the information may be by Federal, State or local governments or agencies, when relevant to civil, criminal, or regulatory investigations or prosecution.

This page intentionally left blank

Designation of Beneficiary

Unpaid Compensation of Deceased Civilian Employee

Important:
Read all instructions before
filling in this form

A. Identification

Name (last, first, middle)		Date of birth (mm, dd, yyyy)	Social Security Number
Department or agency in which presently employed (or former department or agency):			
Department or agency	Bureau	Division	Location (City, state and ZIP code)

I, the employee named above, canceling any and all previous Designations of Beneficiary heretofore made by me, do now designate the beneficiary or beneficiaries named below to receive any **unpaid compensation** due and payable after my death. I understand that this Designation of Beneficiary relates solely to money due as defined in 5 U.S.C. 5581, 5582, 5583, and in no way will affect the disposition of any benefit which may become payable under the Retirement or Group Life Insurance Acts applicable to my Government service. I further understand that this Designation of Beneficiary will remain in full force and effect until (1) I expressly change or revoke it in writing, (2) I transfer to another agency, or (3) I am reemployed by the same or another department or agency of the Government.

B. Information Concerning The Beneficiaries (See Examples of Designations):

First name, middle initial, and last name of each beneficiary	Address (including ZIP code) of each beneficiary	Relationship	Share to be paid to each beneficiary
Date of designation (mm, dd, yyyy)	Your signature		Total = %

C. Witnesses (A witness is not eligible to receive payment as a beneficiary):

We, the undersigned, certify that this statement was signed in our presence.

Signature of witness	Number and street	City, state and ZIP code
Signature of witness	Number and street	City, state and ZIP code

Receiving agency certification

I have reviewed this designation and certify that the designated shares total 100% and that no witnesses are designated as beneficiaries.

Date received	Signature	Date

Type or print your return address to insure return

--

IMPORTANT NOTICE – ORDER OF PRECEDENCE

If there is no designated beneficiary alive at the time of your death, any unpaid compensation owed you (that becomes payable after you die) will be paid to the first person or persons in the order listed below who are alive on the date that entitlement to the payment occurs.

1. To your widow or widower.
2. If neither of the above, to your child or children in equal shares. The share of any deceased child is distributed to the descendants of that child.
3. If none of the above, to your parents in equal shares or the entire amount to the surviving parent.
4. If none of the above, to the duly appointed legal representative of your estate. If there is none, to the person or persons entitled under the laws of the State or other domicile where you lived.

You do not need to designate a beneficiary unless you want to name some person or persons not listed above or you want the payment to be made in a different order.

INSTRUCTIONS

1. The examples on the back of the first page of this form may be helpful to you in filling out this form.
2. Except for signatures, you should type or print all entries in ink (typing is preferred). You should use this form for any designation of beneficiary or beneficiaries. The form must be signed and witnessed.
3. The form should be free of erasures or alterations to avoid a possible legal contest after your death.
4. You do not need to fill out a new form when your name or address changes or when the name or address of your beneficiary changes.
5. You must complete the form in duplicate and file it with your employing agency. To be valid, your agency must receive the completed form prior to your death. The duplicate will be annotated and returned to you as evidence that the original was received and filed with your agency. We suggest that you file the duplicate with your important papers.
6. You can cancel any prior Designation of Beneficiary form without naming a new beneficiary by completing a new form and inserting "Cancel prior designations" in the space provided for the name of beneficiary. This will change the payment to the order of payment described under "Order of Precedence."
7. This designation remains valid unless (a) you change or revoke it, (b) you transfer to another agency, or (c) you leave and then are reemployed by the Federal Government. If you are covered by (b) or (c), you must fill out a new form if you want to change the order of payment described under "Order of Precedence."

NOTE: If this form is not available, any designation, change or cancellation of beneficiary that is witnessed and filed according to these instructions will be valid.

This form is not to be confused with Standard Form 2808, Designation of Beneficiary, Civil Service Retirement System, Standard Form 2823, Designation of Beneficiary, Federal Employees' Group Life Insurance Program, or Standard Form 3102, Designation of Beneficiary, Federal Employees Retirement System.

Privacy Act Statement

Solicitation of this information is authorized by the Code of Federal Regulations, Part 178, Subpart B. The information you furnish will be used to determine the amount, validity, and the person(s) entitled to the unpaid compensation of a deceased Federal employee. The information may be shared and is subject to verification, via paper, electronic media, or through the use of computer matching programs to obtain information necessary for determination of entitlement under this program or to report income for tax purposes. It may also be shared and verified, as noted above, with law enforcement agencies when they are investigating a violation or potential violation of the civil or criminal law. Public Law 104-134 (April 26, 1996) requires that any person doing business with the Federal government furnish a Social Security Number or tax identification number. This is an amendment to title 31, Section 7701. Failure to furnish the requested information may delay or make it impossible for us to determine eligibility of payments.



PAYMENT AUTHORIZATION 2020 Census

PLEASE READ THIS CAREFULLY

On April 26, 1996 the President signed into law legislation mandating the use of Electronic Funds Transfer (EFT) for Federal payments. Specifically, the Debt Collection Improvement Act of 1996 requires that, beginning July 26, 1996, all new employees receive their Federal wages and salaries via EFT. Effective January 2, 1999, the law further requires that all Federal payments be made by EFT including Federal wages and salaries paid to current employees. A waiver may be granted in rare circumstances. Refer to Section 3 to request a waiver.

This form must be completed to determine your appropriate salary payment method per 31 USC 3322, 31 CFR 209 and/or 210. The information is confidential and will be used to process payroll data. Failure to provide the requested information may affect the processing of this form and may delay or prevent the receipt of payments.

Section 1 – YOUR FINANCIAL INSTITUTION

**Complete information about your financial institution in Sections 1 and 2 as required below.
Do not fill out Section 3.**

1. Name of Financial Institution (Your bank or credit union)			
2. Address #1		3. Address #2	
4. City	State	Zip Code	5. Telephone number – Include area code

Section 2 – YOUR ACCOUNT

Complete information about your financial institution in Sections 1 and 2 as required below.

Type of Account – Mark (X) below <input type="checkbox"/> Checking <input type="checkbox"/> Saving	
Routing number – MUST BE 9-DIGIT NUMBER	Confirm Routing number
<div style="display: flex; justify-content: space-between;"> <div style="border-bottom: 1px solid black; width: 100%;"></div> </div>	<div style="display: flex; justify-content: space-between;"> <div style="border-bottom: 1px solid black; width: 100%;"></div> </div>
Note: Call your financial institution for the routing number, or refer to the lower left-hand corner of your check. Account number Confirm Account number	

Section 3 – REQUEST FOR WAIVER

A waiver for the EFT requirement is granted in rare circumstances, however –

- Requesting a waiver means your salary payments will be sent via paper checks;
- Payments via check will delay receipt of payment;
- If your paper check is lost in the mail, you must wait five workdays from the date your check is normally received before submitting a request for a reissued check. Note: The resolution process may take up to six weeks.

If you are still interested in a waiver, please select one or more of the boxes below, in which circumstances are applicable to you. Do not fill out Sections 1 and 2.

I would like to request a waiver because:

- | | | |
|--|---|--|
| <input type="checkbox"/> I do not have a bank account | <input type="checkbox"/> It would impose a financial hardship | <input type="checkbox"/> Of a language barrier |
| <input type="checkbox"/> It would impose a hardship due to mental or physical disability | <input type="checkbox"/> Of a geographic barrier | |

Section 4 – EMPLOYEE CERTIFICATION

I certify that I am entitled to the payment identified above, and that I have read and understand the form. In signing this form, I authorized my payment to be sent to the financial institution named above to be deposited to the designated account.

Employee Signature	Date
--------------------	------

This page intenionally left blank

Form W-4 (2019)

Future developments. For the latest information about any future developments related to Form W-4, such as legislation enacted after it was published, go to www.irs.gov/FormW4.

Purpose. Complete Form W-4 so that your employer can withhold the correct federal income tax from your pay. Consider completing a new Form W-4 each year and when your personal or financial situation changes.

Exemption from withholding. You may claim exemption from withholding for 2019 if **both** of the following apply.

- For 2018 you had a right to a refund of **all** federal income tax withheld because you had **no** tax liability, **and**
- For 2019 you expect a refund of **all** federal income tax withheld because you expect to have **no** tax liability.

If you're exempt, complete **only** lines 1, 2, 3, 4, and 7 and sign the form to validate it. Your exemption for 2019 expires February 17, 2020. See Pub. 505, Tax Withholding and Estimated Tax, to learn more about whether you qualify for exemption from withholding.

General Instructions

If you aren't exempt, follow the rest of these instructions to determine the number of withholding allowances you should claim for withholding for 2019 and any additional amount of tax to have withheld. For regular wages, withholding must be based on allowances you claimed and may not be a flat amount or percentage of wages.

You can also use the calculator at www.irs.gov/W4App to determine your tax withholding more accurately. Consider

using this calculator if you have a more complicated tax situation, such as if you have a working spouse, more than one job, or a large amount of nonwage income not subject to withholding outside of your job. After your Form W-4 takes effect, you can also use this calculator to see how the amount of tax you're having withheld compares to your projected total tax for 2019. If you use the calculator, you don't need to complete any of the worksheets for Form W-4.

Note that if you have too much tax withheld, you will receive a refund when you file your tax return. If you have too little tax withheld, you will owe tax when you file your tax return, and you might owe a penalty.

Filers with multiple jobs or working spouses. If you have more than one job at a time, or if you're married filing jointly and your spouse is also working, read all of the instructions including the instructions for the Two-Earners/Multiple Jobs Worksheet before beginning.

Nonwage income. If you have a large amount of nonwage income not subject to withholding, such as interest or dividends, consider making estimated tax payments using Form 1040-ES, Estimated Tax for Individuals. Otherwise, you might owe additional tax. Or, you can use the Deductions, Adjustments, and Additional Income Worksheet on page 3 or the calculator at www.irs.gov/W4App to make sure you have enough tax withheld from your paycheck. If you have pension or annuity income, see Pub. 505 or use the calculator at www.irs.gov/W4App to find out if you should adjust your withholding on Form W-4 or W-4P.

Nonresident alien. If you're a nonresident alien, see Notice 1392, Supplemental Form W-4 Instructions for Nonresident Aliens, before completing this form.

Specific Instructions

Personal Allowances Worksheet

Complete this worksheet on page 3 first to determine the number of withholding allowances to claim.

Line C. Head of household please note:

Generally, you may claim head of household filing status on your tax return only if you're unmarried and pay more than 50% of the costs of keeping up a home for yourself and a qualifying individual. See Pub. 501 for more information about filing status.

Line E. Child tax credit. When you file your tax return, you may be eligible to claim a child tax credit for each of your eligible children. To qualify, the child must be under age 17 as of December 31, must be your dependent who lives with you for more than half the year, and must have a valid social security number. To learn more about this credit, see Pub. 972, Child Tax Credit. To reduce the tax withheld from your pay by taking this credit into account, follow the instructions on line E of the worksheet. On the worksheet you will be asked about your total income. For this purpose, total income includes all of your wages and other income, including income earned by a spouse if you are filing a joint return.

Line F. Credit for other dependents.

When you file your tax return, you may be eligible to claim a credit for other dependents for whom a child tax credit can't be claimed, such as a qualifying child who doesn't meet the age or social security number requirement for the child tax credit, or a qualifying relative. To learn more about this credit, see Pub. 972. To reduce the tax withheld from your pay by taking this credit into account, follow the instructions on line F of the worksheet. On the worksheet, you will be asked about your total income. For this purpose, total

Separate here and give Form W-4 to your employer. Keep the worksheet(s) for your records.

Form W-4 Department of the Treasury Internal Revenue Service		Employee's Withholding Allowance Certificate		OMB No. 1545-0074
		▶ Whether you're entitled to claim a certain number of allowances or exemption from withholding is subject to review by the IRS. Your employer may be required to send a copy of this form to the IRS.		2019
1 Your first name and middle initial		Last name		2 Your social security number
Home address (number and street or rural route)		3 <input type="checkbox"/> Single <input type="checkbox"/> Married <input type="checkbox"/> Married, but withhold at higher Single rate. Note: If married filing separately, check "Married, but withhold at higher Single rate."		
City or town, state, and ZIP code		4 If your last name differs from that shown on your social security card, check here. You must call 800-772-1213 for a replacement card. ▶ <input type="checkbox"/>		
5 Total number of allowances you're claiming (from the applicable worksheet on the following pages)		5		
6 Additional amount, if any, you want withheld from each paycheck		6 \$		
7 I claim exemption from withholding for 2019, and I certify that I meet both of the following conditions for exemption. • Last year I had a right to a refund of all federal income tax withheld because I had no tax liability, and • This year I expect a refund of all federal income tax withheld because I expect to have no tax liability. If you meet both conditions, write "Exempt" here		7		
Under penalties of perjury, I declare that I have examined this certificate and, to the best of my knowledge and belief, it is true, correct, and complete.				
Employee's signature (This form is not valid unless you sign it.) ▶				
8 Employer's name and address (Employer: Complete boxes 8 and 10 if sending to IRS and complete boxes 8, 9, and 10 if sending to State Directory of New Hires.)		9 First date of employment		10 Employer identification number (EIN)

For Privacy Act and Paperwork Reduction Act Notice, see page 4.

Cat. No. 10220Q

Form **W-4** (2019)

income includes all of your wages and other income, including income earned by a spouse if you are filing a joint return.

Line G. Other credits. You may be able to reduce the tax withheld from your paycheck if you expect to claim other tax credits, such as tax credits for education (see Pub. 970). If you do so, your paycheck will be larger, but the amount of any refund that you receive when you file your tax return will be smaller. Follow the instructions for Worksheet 1-6 in Pub. 505 if you want to reduce your withholding to take these credits into account. Enter “-0-” on lines E and F if you use Worksheet 1-6.

Deductions, Adjustments, and Additional Income Worksheet

Complete this worksheet to determine if you’re able to reduce the tax withheld from your paycheck to account for your itemized deductions and other adjustments to income, such as IRA contributions. If you do so, your refund at the end of the year will be smaller, but your paycheck will be larger. You’re not required to complete this worksheet or reduce your withholding if you don’t wish to do so.

You can also use this worksheet to figure out how much to increase the tax withheld from your paycheck if you have a large amount of nonwage income not subject to withholding, such as interest or dividends.

Another option is to take these items into account and make your withholding more accurate by using the calculator at www.irs.gov/W4App. If you use the calculator, you don’t need to complete any of the worksheets for Form W-4.

Two-Earners/Multiple Jobs Worksheet

Complete this worksheet if you have more than one job at a time or are married filing jointly and have a working spouse. If you

don’t complete this worksheet, you might have too little tax withheld. If so, you will owe tax when you file your tax return and might be subject to a penalty.

Figure the total number of allowances you’re entitled to claim and any additional amount of tax to withhold on all jobs using worksheets from only one Form W-4. Claim all allowances on the W-4 that you or your spouse file for the highest paying job in your family and claim zero allowances on Forms W-4 filed for all other jobs. For example, if you earn \$60,000 per year and your spouse earns \$20,000, you should complete the worksheets to determine what to enter on lines 5 and 6 of your Form W-4, and your spouse should enter zero (“-0-”) on lines 5 and 6 of his or her Form W-4. See Pub. 505 for details.

Another option is to use the calculator at www.irs.gov/W4App to make your withholding more accurate.

Tip: If you have a working spouse and your incomes are similar, you can check the “Married, but withhold at higher Single rate” box instead of using this worksheet. If you choose this option, then each spouse should fill out the Personal Allowances Worksheet and check the “Married, but withhold at higher Single rate” box on Form W-4, but only one spouse should claim any allowances for credits or fill out the Deductions, Adjustments, and Additional Income Worksheet.

Instructions for Employer

Employees, do not complete box 8, 9, or 10. Your employer will complete these boxes if necessary.

New hire reporting. Employers are required by law to report new employees to a designated State Directory of New Hires. Employers may use Form W-4, boxes 8, 9,

and 10 to comply with the new hire reporting requirement for a newly hired employee. A newly hired employee is an employee who hasn’t previously been employed by the employer, or who was previously employed by the employer but has been separated from such prior employment for at least 60 consecutive days. Employers should contact the appropriate State Directory of New Hires to find out how to submit a copy of the completed Form W-4. For information and links to each designated State Directory of New Hires (including for U.S. territories), go to www.acf.hhs.gov/css/employers.

If an employer is sending a copy of Form W-4 to a designated State Directory of New Hires to comply with the new hire reporting requirement for a newly hired employee, complete boxes 8, 9, and 10 as follows.

Box 8. Enter the employer’s name and address. If the employer is sending a copy of this form to a State Directory of New Hires, enter the address where child support agencies should send income withholding orders.

Box 9. If the employer is sending a copy of this form to a State Directory of New Hires, enter the employee’s first date of employment, which is the date services for payment were first performed by the employee. If the employer rehired the employee after the employee had been separated from the employer’s service for at least 60 days, enter the rehire date.

Box 10. Enter the employer’s employer identification number (EIN).

Personal Allowances Worksheet (Keep for your records.)

A	Enter "1" for yourself	A _____
B	Enter "1" if you will file as married filing jointly	B _____
C	Enter "1" if you will file as head of household	C _____
D	Enter "1" if: <ul style="list-style-type: none"> • You're single, or married filing separately, and have only one job; or • You're married filing jointly, have only one job, and your spouse doesn't work; or • Your wages from a second job or your spouse's wages (or the total of both) are \$1,500 or less. 	D _____
E	Child tax credit. See Pub. 972, Child Tax Credit, for more information. <ul style="list-style-type: none"> • If your total income will be less than \$71,201 (\$103,351 if married filing jointly), enter "4" for each eligible child. • If your total income will be from \$71,201 to \$179,050 (\$103,351 to \$345,850 if married filing jointly), enter "2" for each eligible child. • If your total income will be from \$179,051 to \$200,000 (\$345,851 to \$400,000 if married filing jointly), enter "1" for each eligible child. • If your total income will be higher than \$200,000 (\$400,000 if married filing jointly), enter "-0-". 	E _____
F	Credit for other dependents. See Pub. 972, Child Tax Credit, for more information. <ul style="list-style-type: none"> • If your total income will be less than \$71,201 (\$103,351 if married filing jointly), enter "1" for each eligible dependent. • If your total income will be from \$71,201 to \$179,050 (\$103,351 to \$345,850 if married filing jointly), enter "1" for every two dependents (for example, "-0-" for one dependent, "1" if you have two or three dependents, and "2" if you have four dependents). • If your total income will be higher than \$179,050 (\$345,850 if married filing jointly), enter "-0-". 	F _____
G	Other credits. If you have other credits, see Worksheet 1-6 of Pub. 505 and enter the amount from that worksheet here. If you use Worksheet 1-6, enter "-0-" on lines E and F	G _____
H	Add lines A through G and enter the total here	H _____

For accuracy,
complete all
worksheets
that apply.

- If you plan to **itemize** or **claim adjustments to income** and want to reduce your withholding, or if you have a large amount of nonwage income not subject to withholding and want to increase your withholding, see the **Deductions, Adjustments, and Additional Income Worksheet** below.
- If you **have more than one job at a time** or are **married filing jointly and you and your spouse both work**, and the combined earnings from all jobs exceed \$53,000 (\$24,450 if married filing jointly), see the **Two-Earners/Multiple Jobs Worksheet** on page 4 to avoid having too little tax withheld.
- If **neither** of the above situations applies, **stop here** and enter the number from line H on line 5 of Form W-4 above.

Deductions, Adjustments, and Additional Income Worksheet

Note: Use this worksheet only if you plan to itemize deductions, claim certain adjustments to income, or have a large amount of nonwage income not subject to withholding.

1	Enter an estimate of your 2019 itemized deductions. These include qualifying home mortgage interest, charitable contributions, state and local taxes (up to \$10,000), and medical expenses in excess of 10% of your income. See Pub. 505 for details	1 \$ _____
2	Enter: <ul style="list-style-type: none"> \$24,400 if you're married filing jointly or qualifying widow(er) \$18,350 if you're head of household \$12,200 if you're single or married filing separately 	2 \$ _____
3	Subtract line 2 from line 1. If zero or less, enter "-0-".	3 \$ _____
4	Enter an estimate of your 2019 adjustments to income, qualified business income deduction, and any additional standard deduction for age or blindness (see Pub. 505 for information about these items)	4 \$ _____
5	Add lines 3 and 4 and enter the total	5 \$ _____
6	Enter an estimate of your 2019 nonwage income not subject to withholding (such as dividends or interest)	6 \$ _____
7	Subtract line 6 from line 5. If zero, enter "-0-". If less than zero, enter the amount in parentheses	7 \$ _____
8	Divide the amount on line 7 by \$4,200 and enter the result here. If a negative amount, enter in parentheses. Drop any fraction	8 _____
9	Enter the number from the Personal Allowances Worksheet , line H, above	9 _____
10	Add lines 8 and 9 and enter the total here. If zero or less, enter "-0-". If you plan to use the Two-Earners/Multiple Jobs Worksheet , also enter this total on line 1 of that worksheet on page 4. Otherwise, stop here and enter this total on Form W-4, line 5, page 1	10 _____

Two-Earners/Multiple Jobs Worksheet

Note: Use this worksheet only if the instructions under line H from the **Personal Allowances Worksheet** direct you here.

- 1** Enter the number from the **Personal Allowances Worksheet**, line H, page 3 (or, if you used the **Deductions, Adjustments, and Additional Income Worksheet** on page 3, the number from line 10 of that worksheet) **1** _____
 - 2** Find the number in **Table 1** below that applies to the **LOWEST** paying job and enter it here. **However**, if you're married filing jointly and wages from the highest paying job are \$75,000 or less and the combined wages for you and your spouse are \$107,000 or less, don't enter more than "3" **2** _____
 - 3** If line 1 is **more than or equal to** line 2, subtract line 2 from line 1. Enter the result here (if zero, enter "-0-") and on Form W-4, line 5, page 1. **Do not** use the rest of this worksheet **3** _____
- Note:** If line 1 is **less than** line 2, enter "-0-" on Form W-4, line 5, page 1. Complete lines 4 through 9 below to figure the additional withholding amount necessary to avoid a year-end tax bill.
- 4** Enter the number from line 2 of this worksheet **4** _____
 - 5** Enter the number from line 1 of this worksheet **5** _____
 - 6** **Subtract** line 5 from line 4 **6** _____
 - 7** Find the amount in **Table 2** below that applies to the **HIGHEST** paying job and enter it here **7** \$ _____
 - 8** **Multiply** line 7 by line 6 and enter the result here. This is the additional annual withholding needed **8** \$ _____
 - 9** **Divide** line 8 by the number of pay periods remaining in 2019. For example, divide by 18 if you're paid every 2 weeks and you complete this form on a date in late April when there are 18 pay periods remaining in 2019. Enter the result here and on Form W-4, line 6, page 1. This is the additional amount to be withheld from each paycheck **9** \$ _____

Table 1				Table 2			
Married Filing Jointly		All Others		Married Filing Jointly		All Others	
If wages from LOWEST paying job are—	Enter on line 2 above	If wages from LOWEST paying job are—	Enter on line 2 above	If wages from HIGHEST paying job are—	Enter on line 7 above	If wages from HIGHEST paying job are—	Enter on line 7 above
\$0 - \$5,000	0	\$0 - \$7,000	0	\$0 - \$24,900	\$420	\$0 - \$7,200	\$420
5,001 - 9,500	1	7,001 - 13,000	1	24,901 - 84,450	500	7,201 - 36,975	500
9,501 - 19,500	2	13,001 - 27,500	2	84,451 - 173,900	910	36,976 - 81,700	910
19,501 - 35,000	3	27,501 - 32,000	3	173,901 - 326,950	1,000	81,701 - 158,225	1,000
35,001 - 40,000	4	32,001 - 40,000	4	326,951 - 413,700	1,330	158,226 - 201,600	1,330
40,001 - 46,000	5	40,001 - 60,000	5	413,701 - 617,850	1,450	201,601 - 507,800	1,450
46,001 - 55,000	6	60,001 - 75,000	6	617,851 and over	1,540	507,801 and over	1,540
55,001 - 60,000	7	75,001 - 85,000	7				
60,001 - 70,000	8	85,001 - 95,000	8				
70,001 - 75,000	9	95,001 - 100,000	9				
75,001 - 85,000	10	100,001 - 110,000	10				
85,001 - 95,000	11	110,001 - 115,000	11				
95,001 - 125,000	12	115,001 - 125,000	12				
125,001 - 155,000	13	125,001 - 135,000	13				
155,001 - 165,000	14	135,001 - 145,000	14				
165,001 - 175,000	15	145,001 - 160,000	15				
175,001 - 180,000	16	160,001 - 180,000	16				
180,001 - 195,000	17	180,001 and over	17				
195,001 - 205,000	18						
205,001 and over	19						

Privacy Act and Paperwork Reduction Act Notice. We ask for the information on this form to carry out the Internal Revenue laws of the United States. Internal Revenue Code sections 3402(f)(2) and 6109 and their regulations require you to provide this information; your employer uses it to determine your federal income tax withholding. Failure to provide a properly completed form will result in your being treated as a single person who claims no withholding allowances; providing fraudulent information may subject you to penalties. Routine uses of this information include giving it to the Department of Justice for civil and criminal litigation; to

cities, states, the District of Columbia, and U.S. commonwealths and possessions for use in administering their tax laws; and to the Department of Health and Human Services for use in the National Directory of New Hires. We may also disclose this information to other countries under a tax treaty, to federal and state agencies to enforce federal nontax criminal laws, or to federal law enforcement and intelligence agencies to combat terrorism.

You aren't required to provide the information requested on a form that's subject to the Paperwork Reduction Act unless the form displays a valid OMB control number. Books or records relating

to a form or its instructions must be retained as long as their contents may become material in the administration of any Internal Revenue law. Generally, tax returns and return information are confidential, as required by Code section 6103.

The average time and expenses required to complete and file this form will vary depending on individual circumstances. For estimated averages, see the instructions for your income tax return.

If you have suggestions for making this form simpler, we would be happy to hear from you. See the instructions for your income tax return.



MOST FREQUENTLY ASKED QUESTIONS BY EMPLOYEES

2020 Census

Reference – Census Employee Handbook, Chapter 3: Personnel and Payroll

What type of appointment am I on?

You are appointed to a time limited temporary appointment with a specific expiration date. Your work schedule is intermittent. This means you have no set schedule tour of duty. You will only work when assignments are available. After work is completed, your employment may be terminated, even if your appointment has not expired.

Am I entitled to any health or life benefits or leave?

You are eligible for health benefits if you meet one of the following thresholds:

- 1) Employees on temporary appointments limited to 1 year (or less) who have worked or are expected to work at least 90 days and have worked or are expected to work 130 or more hours (i.e., work and paid leave, as well as qualifying leave-without-pay hours) per calendar month (equivalent to 30 hours per week); and
- 2) Employees under a seasonal or intermittent work schedule (regardless of appointment type or length of appointment) who have worked or are expected to work at least 90 days and have worked or are expected to work 130 or more hours (i.e., work and paid leave, as well as qualifying leave-without-pay hours) per calendar month (equivalent to 30 hours per week).

You are not eligible to earn annual or sick leave nor are you eligible for life insurance benefits.

When will I receive my first paycheck and subsequent checks?

You will receive your first paycheck approximately 11 days after you complete your first workweek. Thereafter, you will be paid every Wednesday for each week that you work.

Am I required by law to have my check direct deposited?

Yes, the Department of Treasury passed a law on January 1, 1999 that requires all federal payments to be issued electronically into your checking/savings account at your financial institution. We encourage all employees to have Direct Deposit. It is fast and safe—there is never any chance of lost or stolen funds. You and your financial institution must complete the D-1199, Direct Deposit Authorization, and submit it to your supervisor or mail it directly to your area census office. If you do not sign up for Direct Deposit, your check can be mailed to an address specified by you, after completing a Form D-260, Waiver of Electronic Salary Payment.

Can I change my tax withholding at a later date?

Yes, you must fill out the applicable federal or state tax withholdings form(s), or submit a signed document requesting the change to your area census office.

Am I paid for my lunch break or other breaks from census work?

No, you are not paid for breaks. If you are on official duty and take a break/lunch break, do not record this time as paid time on your payroll document. You are only paid for the hours that you actually work.

What kind of official work expenses can I be reimbursed for?

You can be reimbursed for any expenses that you incur while performing official census business duties, i.e., mileage, official telephone calls, and parking. These reimbursements are not taxable items and in some situations receipts and supervisor approval are required.

How do I report my hours worked and my reimbursable expenses?

You will need to complete the Form E-308, *Electronic Daily Pay and Work Record* and submit it to your supervisor for each day you work. If you do not work a day, you do not need to complete a E-308.

Am I able to work overtime to complete my work?

Overtime is not permitted without approval from your supervisor. If your supervisor determines that it is necessary that overtime hours should be authorized and there is no other viable solution but to work overtime, then they will seek authorization from the appropriate manager or designee and let you know if you should work the overtime hours. **Do not work overtime without PRIOR APPROVAL from your supervisor.** If you work overtime without prior approval, you will be terminated. For more information on overtime, refer to your Census Employee Handbook.

If I don't receive my paycheck within 3 days of the scheduled pay date, or, if I have questions regarding my appointment or other pay issues, who do I contact?

If you have an administrative or payroll problem of any kind you should contact the Decennial Service Center (DSC) at 1-855-236-2020 option #2. This number is not intended for reporting grievances or other unresolved workplace issues.

Who can I talk to about unresolved workplace issues?

If there are any outstanding issues that you have been unable to resolve with local and Regional Census Center management, you can call the Census Equal Employment Opportunity (EEO) Hotline at 1-800-872-6096.



U.S. DEPARTMENT OF COMMERCE
Economics and Statistics Administration
U.S. CENSUS BUREAU

PERSONAL TELEPHONE REIMBURSEMENT POLICY AGREEMENT FOR 2020 Census

NOTICE

Please read this statement carefully and discuss any questions you may have with your servicing office at 1-855-562-2020, option 3, before signing it and acknowledging your understanding of the policy.

POLICY

As stated in the **Census Employees Handbook** (D-590), Chapter 3, Topic 4, Reimbursement Expenses:

The Census Bureau will reimburse you for official census duty business related local and long-distance calls made from your home, cellular, or a public telephone, in excess of your existing plan or excess that was caused by Census-related calls. The Census Bureau will not reimburse you for personal phone calls. However, if you were issued a government phone, you are expected to use the government issued phone to make census-related business calls. In this instance you should not use your own home, cell or a public phone (unless there is an issue with your government issued phone not working properly). Only employees who work on the site and were not issued a government phone should claim reimbursement for home, cell or public phone charges.

STATEMENT OF UNDERSTANDING

I understand that I can claim reimbursement for official Census business related telephone calls made from my personal phone that exceed my standard or basic service or business related telephone calls made from a prepaid wireless plan, phone card or flat rate plan. The Census Bureau will not reimburse me for charges that are covered by my basic service plan. The Census Bureau will not pay for the basic service plan itself, or any changes that I make to my basic service plan. Additionally, the Census Bureau has established a CAP for reimbursement of \$240/month. Use of my personal phone for Census business related calls is voluntary.

I agree to submit an itemized copy of my telephone bill that verifies the total of reimbursable expenses that I enter on my payroll form.

CERTIFICATION

I have read, fully understand, and agree to the procedures regarding approval for telephone reimbursement. I understand that failure to follow the policy and procedures will result in my reimbursement claim not being processed or paid. Falsification of charges is grounds for removal.

Signature of employee

Date

Full name of employee – Please print.

USE OF PERSONAL CELL PHONES

1. When practical, use your personal land line for making business related calls. This will reduce the number of minutes used against your cell phone plan.
2. When having to use your cell phone, use during evenings and weekends when plans provide free minutes; it is advantageous to you and the Census Bureau. The same applies to within plan calls (e.g., Verizon to Verizon, or Sprint to Sprint).
3. For the ACO staff, cell phone use should be limited to setting up or confirming the daily meetings. Long conversations should be saved for when the parties meet in person.
4. The Census Bureau does not pay for roaming charges.
5. The Census Bureau does not pay for the phone, service plan, any additional devices (e.g., car chargers or the like) or additional services like text messaging, pictures, ring tones, screen savers, web access, call transfers, or the like.
6. Under no circumstances should you use your cell phone when driving a car without a hands-free device in place and operational. Without a hands-free device, you should find a safe place to park then make your call. You should never text while driving.
7. If the charges claimed are for cell phone usage (versus home or public phone), the employee will only be reimbursed for the minutes of calls made for official business only. However, an employee is only eligible for reimbursement if he/she goes over the monthly minutes allocated in their plan. Since business minutes used within the plan allowance may be the reason for going over the monthly minutes allocated in the plan, the employee can use those business minutes in calculating the reimbursement.

To calculate the amount the employee will be reimbursed for any one month, perform the following steps.

- a. Determine the total number of minutes (business and personal) that the employee was charged over the minutes allocated in the plan. This is X.
 - b. Determine the total number of business related minutes the employee used. Include the business minutes used that are within the monthly allowance of the plan and over the plan. This is Y.
 - c. Determine which is the lesser amount between X and Y.
 - d. Multiply the lesser amount (X or Y) times the overage rate. For example, the overage rate may be 40 cents per minute. The overage rate will be shown on the itemized bill.
8. There are specific procedures for claiming reimbursement of business related calls that are in excess of the service plan. They require (among other things):
 - a. An itemized bill, checking off or circling every business related call
 - b. Addition of all the minutes related to business calls
 - c. Comparison of Minutes used this month to Total Minutes allocated in the Plan to Total Minutes of Business Related Calls
 - d. Supervisory review and signatory approval of the claimed reimbursement
 - e. Claim totals in the appropriate area of the signed and approved Work Record or Cost Report with a copy of the itemized bill attached
 9. There are similar procedures for reimbursing employees for business related calls made on a pre-paid wireless plan, phone card or flat rate plan.
 10. The Census Bureau has the right to limit the monthly amount of reimbursement (capped at \$240) for business related calls, based on funding limitations.



WHAT YOU MUST DO TO GET YOUR PAYCHECK ON TIME ADMINISTRATIVE RESPONSIBILITIES FOR ALL EMPLOYEES 2020 Census

ADMINISTRATIVE RESPONSIBILITIES FOR ALL EMPLOYEES

Below are some of the administrative activities that YOU are responsible for during the duration of your employment with the U.S. Census Bureau. Following these guidelines ensures that the processing of your hire action and payroll information will be timely and accurate. Most administrative problems or questions can be resolved by first contacting your immediate supervisor and then your ACO administrative section. If you find that you still need further assistance, contact the Decennial Service Center (DSC) at 1-855-236-2020, option #3.

PERSONNEL FORMS

- Make sure you complete all onboarding documents before operational training.
- Enter the effective date of your hire action and take the Oath of Office on Form BC-61, Appointment Affidavits, to become an official census employee.
- Carefully review current information on Form D-155, Applicant Data Sheet, (especially your name, Social Security Number, and home/mailling address). Correct any information that has changed or is in error, and sign your initials next to the corrected information.
- Ensure that all personnel documents are signed, dated, and all entries are legible.
- Ensure that all new hire forms are completed, put into your appointment folder and returned to the trainer during operational training.

PAYROLL

▶ E-308

- Complete an E-308, Electronic Daily Pay and Work Record, for every day you work and transmit it **daily** to your supervisor.
- After reviewing the information is accurate, attest each E-308.
- If you are an enumerator, ensure your supervisor approves your E-308s daily.

NOTE

It is extremely important that you work closely with your supervisor to review each submitted E-308. Your supervisor will submit the E-308s to the office **daily**. The information you provide will assist census managers in monitoring and conducting the 2020 Census, and ensure you get your paycheck on schedule as expected.

This Page Intentionally Left Blank

Appendix B: Rules and Regulations Governing Conduct on Federal Property

Rules and Regulations Governing Conduct on Federal Property

November, 2005

Federal Management Regulation Title 41, Code of Federal Regulations, Part 102-74, Subpart C

Applicability (41 CFR 102-74.365). The rules in this subpart apply to all property under the authority of GSA and to all persons entering in or on such property. Each occupant agency shall be responsible for the observance of these rules and regulations. Federal agencies must post the notice in the Appendix to this part at each public entrance to each Federal facility.

Inspection (41 CFR 102-74.370). Federal agencies may, at their discretion, inspect packages, briefcases and other containers in the immediate possession of visitors, employees or other persons arriving on, working at, visiting, or departing from Federal property. Federal agencies may conduct a full search of a person and the vehicle the person is driving or occupying upon his or her arrest.

Admission to Property (41 CFR 102-74.375). Federal agencies must:

- Except as otherwise permitted, close property to the public during other than normal working hours. In those instances where a Federal agency has approved the after-normal-working hours use of buildings or portions thereof for activities authorized by subpart D of this part, Federal agencies must not close the property for affected portions thereof to the public;
- Close property to the public during working hours only when situations require this action to ensure the orderly conduct of Government business. The designated official under the Occupant Emergency Program may make such decision only after consultation with the buildings manager and the highest ranking representative of the law enforcement organization responsible for protection of the property or the area. The designated official is defined in Sec. 102-71.20 of this chapter as the highest ranking official of the primary occupant agency, or the alternate highest ranking official or designee selected by mutual agreement by other occupant agency officials; and
- When property or a portion thereof is closed to the public, restrict admission to the property, or the affected portion, to authorized persons who must register upon entry to the property and must, when requested, display Government or other identifying credentials to Federal police officers or other authorized individuals when entering, leaving or while on the property. Failure to comply with any of the applicable provisions is a violation of these regulations.

Preservation of Property (41 CFR 102-74.380). All persons entering in or on Federal property are prohibited from:

- Improperly disposing of rubbish on property;
- Willfully destroying or damaging property;
- Stealing property;
- Creating any hazard on property to persons or things; or
- Throwing articles of any kind from or at a building or discharging upon statues, fountains or any part of the building.

Conformity with Signs and Directions (41 CFR 102-74.385). Persons in and on property must at all times comply with official signs of a prohibitory, regulatory or directory nature and with the lawful direction of Federal police officers and other authorized individuals.

Disturbances (41 CFR 102-74.390). All persons entering

in or on Federal property are prohibited from loitering, exhibiting disorderly conduct or exhibiting other conduct on property that:

- Creates loud or unusual noise or a nuisance;
- Unreasonably obstructs the usual use of entrances, lobbies, corridors, offices, elevators, stairways, or parking lots;
- Otherwise impedes or disrupts the performance of official duties by Government employees; or
- Prevents the general public from obtaining the administrative services provided on the property in a timely manner.

Gambling (41 CFR 102-74.395). (a) Except for the vending or exchange of chances by licensed blind operators of vending facilities for any lottery set forth in a State law and authorized by section 2(a)(5) of the Randolph-Sheppard Act (20 U.S.C. 107 et seq.), all persons entering in or on Federal property are prohibited from:

- Participating in games for money or other personal property;
 - Operating gambling devices;
 - Conducting a lottery or pool; or
 - Selling or purchasing numbers tickets.
- (b) This provision is not intended to prohibit prize drawings for personal property at otherwise permitted fundations on Federal property, provided that the game or drawing does not constitute gambling per se. Gambling per se means a game of chance where the participant risks something of value for the chance to gain or win a prize.

Narcotics and Other Drugs (41 CFR 102-74.400). Except in cases where the drug is being used as prescribed for a patient by a licensed physician, all persons entering in or on Federal property are prohibited from:

- Being under the influence, using or possessing any narcotic drugs, hallucinogens, marijuana, barbiturates, or amphetamines; or
- Operating a motor vehicle on the property while under the influence of alcoholic beverages, narcotic drugs, hallucinogens, marijuana, barbiturates, or amphetamines.

Alcoholic Beverages (41 CFR 102-74.405). Except where the head of the responsible agency or his or her designee has granted an exemption in writing for the appropriate official use of alcoholic beverages, all persons entering in or on Federal property are prohibited from being under the influence or using alcoholic beverages. The head of the responsible agency or his or her designee must provide a copy of all exemptions granted to the buildings manager and the highest ranking representative of the law enforcement organization, or other authorized officials, responsible for the security of the property.

Soliciting, Vending and Debt Collection (41 CFR 102-74.410). All persons entering in or on Federal property are prohibited from soliciting alms (including money and non-monetary items) or commercial or political donations, vending merchandise of all kinds, displaying or distributing commercial advertising, or collecting private debts, except for:

- National or local drives for funds for welfare, health or other purposes as authorized by 5 CFR part 950, entitled "Solicitation of Federal Civilian and Uniformed Service Personnel for Contributions to Private Voluntary Organizations," and sponsored or approved by the occupant agencies;
- Concessions or personal notices posted by employees on authorized bulletin boards;
- Solicitation of labor organization membership or dues authorized by occupant agencies under the Civil Service Reform Act of 1978 (Pub. L. 95-454);
- Lessee, or its agents and employees, with respect to space leased for commercial, cultural, educational, or recreational use under 40 U.S.C. 581(h). Public areas of GSA-controlled property may be used for other activities in accordance with subpart D of this part;
- Collection of non-monetary items that are sponsored or approved by the occupant agencies; and
- Commercial activities sponsored by recognized Federal employee associations and on-site child care centers.

Posting and Distributing Materials (41 CFR 102-74.415). All persons entering in or on Federal property are prohibited from:

- Distributing free samples of tobacco products in or around Federal buildings, as mandated by Section 636 of Public Law 104-52;
- Posting or affixing materials, such as pamphlets, handbills, or flyers, on bulletin boards or elsewhere on GSA-controlled property, except as authorized in Sec. 102-74.410, or when these displays are conducted as part of authorized Government activities; and
- Distributing materials, such as pamphlets, handbills or flyers, unless conducted as part of authorized Government activities. This prohibition does not apply to public areas of the property as defined in Sec. 102-71.20 of this chapter. However, any person or organization proposing to distribute materials in a public area under this section must first obtain a permit from the building manager as specified in subpart D of this part. Any such person or organization must distribute materials only in accordance with the provisions of subpart D of this part. Failure to comply with these provisions is a violation of these regulations.

Photographs for News, Advertising, or Commercial Purposes (41 CFR 102-74.420). Except where security regulations, rules, orders, or directives apply or a Federal court order or rule prohibits it, persons entering in or on Federal property may take photographs of:

- Space occupied by a tenant agency for non-commercial purposes only with the permission of the occupying agency concerned;
- Space occupied by a tenant agency for commercial purposes only with written permission of an authorized official of the occupying agency concerned; and
- Building entrances, lobbies, lobbies, corridors, or auditoriums for news purposes.

Dogs and Other Animals (41 CFR 102-74.425). No person may bring dogs or other animals on Federal property for other than official purposes. However, a disabled person may bring

a seeing-eye dog, a guide dog, or other animal assisting or being trained to assist that individual.

Breastfeeding (41 CFR 102-74.426). Public Law 108-139, Section 629, Division F, Title VI (January 23, 2004), provides that a woman may breastfeed her child at any location in a Federal building or on Federal property, if the woman and her child are otherwise authorized to be present at the location.

Vehicle and Pedestrian Traffic (41 CFR 102-74.430). All vehicle drivers entering or while on Federal property:

- Must drive in a careful and safe manner at all times;
- Must comply with the signals and directions of Federal police officers or other authorized individuals;
- Must comply with all posted traffic signs;
- Must comply with any additional posted traffic directives approved by the GSA Regional Administrator, which will have the same force and effect as these regulations;
- Are prohibited from blocking entrances, driveways, walks, loading platforms, or fire hydrants; and
- Are prohibited from parking on Federal property without a permit. Parking without authority, parking in unauthorized locations or in locations reserved for other persons, or parking contrary to the direction of posted signs is prohibited. Vehicles parked in violation, where warning signs are posted, are subject to removal at the owner's risk and expense. Federal agencies may take as proof that a motor vehicle was parked in violation of these regulations or directives as prima facie evidence that the registered owner was responsible for the violation.

Explosives (41 CFR 102-74.435). No person entering or while on Federal property may carry or possess explosives, or items intended to be used to fabricate an explosive or incendiary device, either openly or concealed, except for official purposes.

Weapons (41 CFR 102-74.440). Federal law prohibits the possession of firearms and other dangerous weapons in Federal facilities and Federal court facilities by all persons not specifically authorized by 18 U.S.C. 930. Violators will be subject to fine and/or imprisonment for periods up to five (5) years.

Nondiscrimination (41 CFR 102-74.445). Federal agencies must not discriminate by segregation or otherwise against any person or persons because of race, creed, religion, age, sex, color, disability, or national origin in furnishing or by refusing to furnish to such person or persons the use of any facility of a public nature, including all services, privileges, accommodations, and activities provided on the property.

Penalties (41 CFR 102-74.450). A person found guilty of violating any rule or regulation in this subpart while on any property under the charge and control of GSA shall be fined under title 18 of the United States Code, imprisoned for not more than 30 days, or both.

Impact on Other Laws or Regulations (41 CFR 102-74.455). No rule or regulation in this subpart may be construed to nullify any other Federal laws or regulations or any State and local laws and regulations applicable to any area in which the property is situated (40 U.S.C. 121(c)).

WARNING WEAPONS PROHIBITED

Federal law prohibits the possession of firearms or other dangerous weapons in Federal facilities and Federal court facilities by all persons not specifically authorized by Title 18, United States Code, Section 930. Violators will be subject to fine and/or imprisonment for periods up to five (5) years.

Special Note

The U.S. Census Bureau will not condone, encourage or otherwise allow field employees to carry firearms or other weapons while performing their official duties. The U.S. Census Bureau will not officially allow the carriage of pepper spray or other chemical projectors while on official government business. If the carriage of chemical projectors is permissible by local law and an individual owns and carries a commercially available product, that is a personal decision. The use of any such device will be a personal decision with any criminal or civil liability accruing to the individual. The U.S. Census Bureau will not support or represent an individual as an employee performing official duties in a case involving the use of a chemical projector.

Appendix C: Records Management Training

2020 Records Management Training for Census Employees and Contractors

1.1 Course Introduction



2020 Records Management Training for Census Employees and Contractors

1.2 Welcome



Welcome to the 2020 Records Management Training For Census Employees & Contractors

1.3 About this Course



About This Course

This course is designed to help you understand the basic responsibilities for managing Federal records, in accordance with laws, policies and procedures that govern Federal records management.

To receive credit for the course you must complete the entire lesson and successfully complete the knowledge check at the end of the course. You must also complete the end-of-course evaluation.

Page 3

About This Course

This course is designed to help you understand the basic responsibilities for managing Federal records, in accordance with laws, policies and procedures that govern Federal records management.

To receive credit for the course you must complete the entire lesson and successfully complete the knowledge check at the end of the course. You must also complete the end-of-course evaluation.

1.4 Objective slide

The slide features a title box with the text "Course Objectives" in blue, outlined with a multi-colored border. Below the title, a text box states "Upon completion of this course, you will be able to:" followed by a smaller box with the instruction "Click the icons above to learn more". There are four circular icons arranged in a 2x2 grid: a yellow circle with a black factory icon, a green circle with a black group of people icon, a blue circle with a black document icon, and a red circle with a black folder icon. To the right of the icons is a photograph of a smiling woman in a grey blazer, with a magnifying glass icon overlaid on her shoulder. The bottom right corner of the slide has a purple bar with the text "Page 4".

Course Objectives

Upon completion of this course, you will be able to:

Identify procedures for managing records containing sensitive information.

Describe your responsibilities regarding records.

Determine what constitutes a
Federal Record.

Identify the fundamentals of managing records.

1.5 Objective slide

The slide features a title box with the text "Let's Get Started" in blue, outlined with a multi-colored border. The background of the slide is a photograph of a diverse group of business professionals in an office setting. Some are standing and talking, while others are sitting at a table with laptops and documents. The bottom right corner of the slide has a purple bar with the text "Page 5".

Let's Get Started

1.6 Objective slide



Why Records Management?

Effective management of records:

- Helps agencies meet statutory and regulatory requirements
- Contributes to the smooth operation of Agency programs
- Helps deliver services in a consistent and equitable manner
- Facilitates the effective performance of program activities
- Protects citizens, businesses and the Census Bureau
- Provides continuity in the event of a disaster
- Protects information from inappropriate/unauthorized access

Page 6

Why Records Management?

Effective management of records:

- Helps agencies meet statutory and regulatory requirements
- Contributes to the smooth operation of Agency programs
- Helps deliver services in a consistent and equitable manner
- Facilitates the effective performance of program activities
- Protects citizens, businesses and the Census Bureau
- Provides continuity in the event of a disaster
- Protects information from inappropriate/unauthorized access

1.7 It's The Law



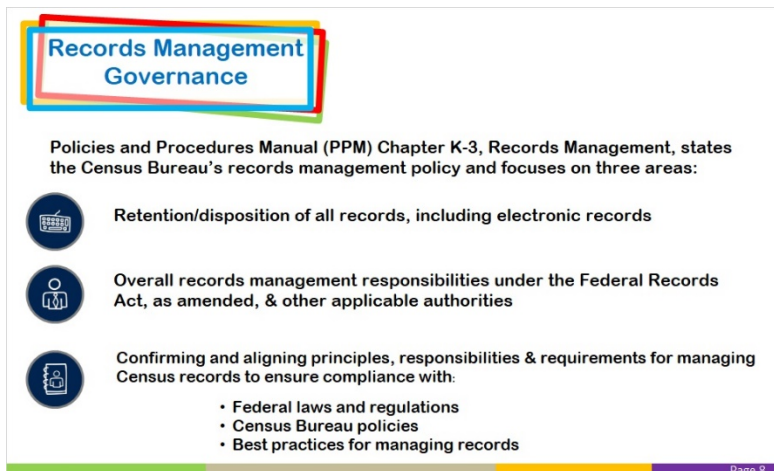
It's The Law

Census Employees and Contractors are required to:

- The Federal Records Act of 1950 (44 U.S.C Ch. 31) - Record Management by Federal Agencies
- 44 U.S.C Chapter 33 - Disposal of Records
- Title 5, Title 13, and Title 26. According to the US Federal Code and the Code of Federal Regulations, everyone is responsible for managing records

1. Manage information that documents work performed
2. Safeguard information that needs to be protected
3. Keep or dispose of records according to approved records schedule

1.8 Objective slide



Records Management Governance

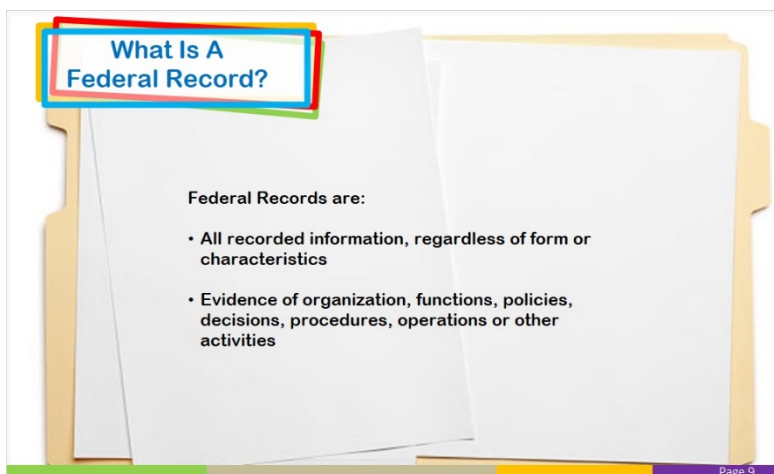
Policies and Procedures Manual (PPM) Chapter K-3, Records Management, states the Census Bureau's records management policy and focuses on three areas:

- Retention/disposition of all records, including electronic records
- Overall records management responsibilities under the Federal Records Act, as amended, & other applicable authorities
- Confirming and aligning principles, responsibilities & requirements for managing Census records to ensure compliance with:
 - Federal laws and regulations
 - Census Bureau policies
 - Best practices for managing records

Page 8

Records Management Governance

- Policies and Procedures Manual (PPM) Chapter K-3, Records Management, states the Census Bureau's records management policy and focuses on three areas:
- Retention/disposition of all records, including electronic records
- Overall records management responsibilities under the Federal Records Act, as amended, & other applicable authorities
- Confirming and aligning principles, responsibilities & requirements for managing Census records to ensure compliance with:
 - Federal laws and regulations
 - Census Bureau policies
 - Best practices for managing records



What Is A Federal Record?

Federal Records are:

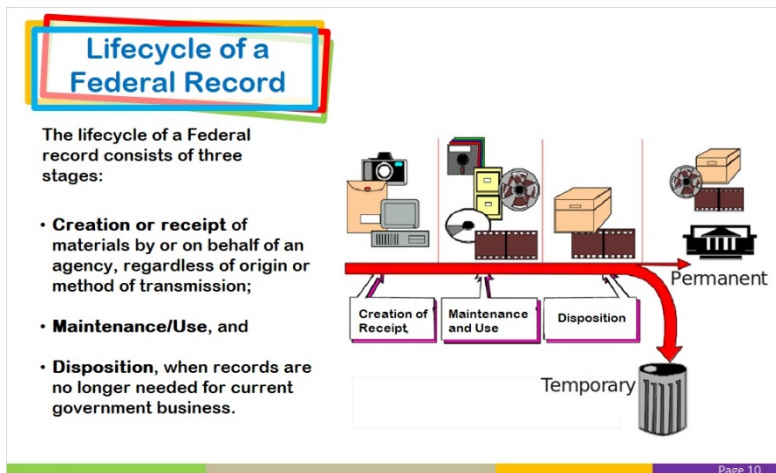
- All recorded information, regardless of form or characteristics
- Evidence of organization, functions, policies, decisions, procedures, operations or other activities

Page 9

What Is A Federal Record?

Federal Records are:

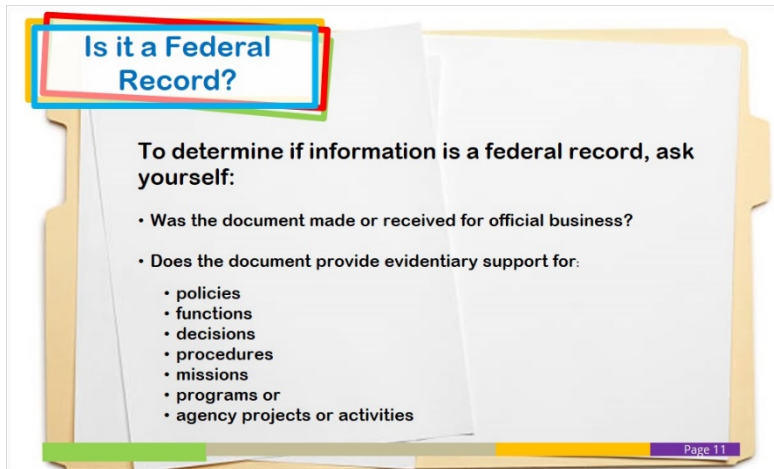
- All recorded information, regardless of form or characteristics
Evidence of organization, functions, policies, decisions, procedures, operations or other activities
- Evidence of organization functions, policies, decisions, procedures, operations or other activities



Lifecycle of a Federal Record

The lifecycle of a Federal record consists of three stages:

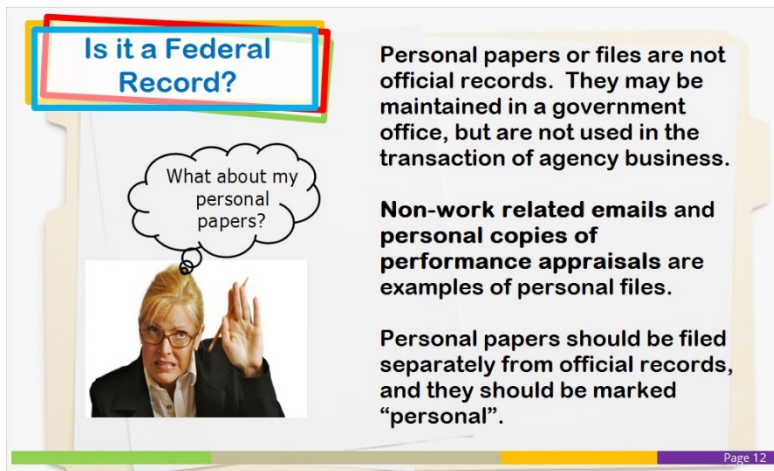
- **Creation or receipt** of materials by or on behalf of an agency, regardless of origin or method of transmission;
- **Maintenance/Use**, and
- **Disposition**, when records are no longer needed for current government business.



Is it a Federal Record?

To determine if information is a federal record, ask yourself:

- Was the document made or received for official business?
- Does the document provide evidentiary support for:
 - Policies
 - Functions
 - Decisions
 - Procedures
 - Missions
 - programs or agency projects or activities



Is it a Federal Record?

What about my personal papers?

Personal papers or files are not official records. They may be maintained in a government office, but are not used in the transaction of agency business.

Non-work related emails and personal copies of performance appraisals are examples of personal files.

Personal papers should be filed separately from official records, and they should be marked "personal".

Page 12

Is it a Federal Record?


What about my personal papers?

- Personal papers or files are not official records. They may be maintained in a government office, but are not used in the transaction of agency business.
- **Non-work related emails and personal copies of performance appraisals** are examples of personal files.
- Personal papers should be filed separately from official records, and they should be marked "personal".

Caring For Records

To ensure proper care of records:

- Keep records organized and stored in a way that protects the record
- Follow agency policies for storing, signing out, and using records
- Limit unnecessary copies, especially for electronic files
- Separate records and non-records
- Keep personal materials separate from records
- Federal records created while teleworking should be stored in your official file system



Page 13

Caring For Records

To ensure proper care of records:

- Keep records organized and stored in a way that protects the record
- Follow agency policies for storing, signing out, and using records
- Limit unnecessary copies, especially for electronic files
- Separate records and non-records
- Keep personal materials separate from records
- Federal records created while teleworking should be stored in your official file system

Record Schedule

Records Schedules describe Agency records, establish time periods for retention, and provide mandatory disposition instructions when records are no longer needed for current government business.

Records Schedule Item

Sequence Number: 1

Program Management Files

Disposition Authority Number: DAA-0026-2016-0002-0001

Organized by official and then under by type of record. Includes one or more of the following: (a) event files, including minutes, notes, remarks, and correspondence related to attendance at committee meetings, conferences, news briefings, public hearings, and similar events; (b) speeches and testimony, including official speeches and addresses, press conference transcripts, testimony, and presentations at official hearings, functions, or ceremonies; (c) subject files, including correspondence, reports, and other records documenting the origin, planning, content, procedures, results, and effects of the decennial census and its related operations, programs, and plans of the Census Bureau; and (d) scheduling calendars, including calendars, appointment books, and other records containing information related to official activities.

Final Disposition: Permanent

Item Status: Active

Is this item made ready? Yes

Do any of the records covered by this item contain or need to contain information that is not in the public domain? No

SPS or Approved Authority: N1-20-09-211a, N1-20-09-212a, N1-20-09-213a, N1-20-09-214a

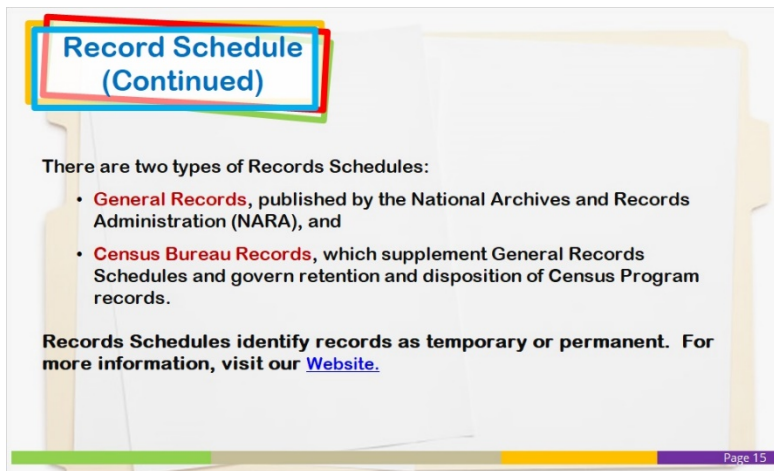
Disposition Instruction: Cross file at the end of each term of office. Transfer paper records to the Census temporary records storage room. Transfer to the National Archives 15 years after release.

Additional Information: What will be the date span of the record transfer of records to the National Archives? Unknown

Page 14

Records Schedule

- Records Schedules describe Agency records, establish time periods for retention, and provide mandatory disposition instructions when records are no longer needed for current government business.

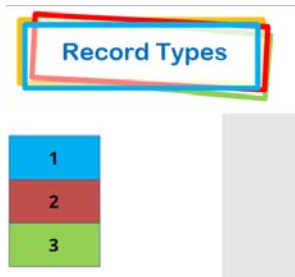


Records Schedule (Continued)

There are two types of Records Schedules:

- General Records, published by the National Archives and Records Administration (NARA), and
- Census Bureau Records, which supplement General Records Schedules and govern retention and disposition of Census Program records.

Records Schedules identify records as temporary or permanent. For more information, visit our [Website](#).

**Record Types**

Permanent Records are appraised by NARA as having sufficient value to warrant continued preservation by the Federal Government as part of the U.S. National Archives.

Permanent Records can include:

- Executive correspondence
- Directives & policy documents
- Official reports & decisions
- High-level committee files
- Organizational charts
- Delegation of authority manuals

Temporary records do not have sufficient value to justify permanent retention and are destroyed.

Temporary records may include:

- Time and attendance files
- Employee travel documents
- Procurement files
- Budget files, and/or
- General accounting files

The Census Bureau can dispose of records identified as “temporary” in accordance with Records Schedules.

A non-record is government owned informational material that is not included in the legal definition of records

Non-records include:

- Personal papers
- Magazines
- Journals
- Copies of documents kept for convenience of reference
- Stocks of publications, library or museum materials used solely for reference or exhibition (Check)

File Inventory					
File Inventory spreadsheet highlights the specific information that is documented on the file inventory. Mandatory entries on the file inventory spreadsheet are Office Name, Series Title, Series Description, Series Location, Inclusive Date, Media Type and Arrangement Date					
Series Title	Series Description	Series Location	Inclusive Date	Media Type	Arrangement
Name of the File	Short description of the Record	Exactly where the record is located	Date range of the Record	Types of Record	How the Record is filed
EXAMPLES					
Time and Attendance	Records of Payroll/ Leave Requests / Sign in Sheets and records pertaining to time and attendance of employee	File Cabinet 4 outside 31234	1/2015 to date	Paper	Alphabetically
Office Files	Routine Administrative Office Files	File Cabinet 2 outside 31234	1/2010 to date	Paper	Alphabetically by subject

Page 17

File Inventory

- File Inventory spreadsheet highlights the specific information that is documented on the file inventory. Mandatory entries on the file inventory spreadsheet are Office Name, Series Title, Series Description, Series Location, Inclusive Date, Media Type and Arrangement Date

Filing Records

Let's take a look at the Census Office File Plan template. Mandatory entries in the file plan are Office Name, Type of Record, Disposition Instructions, Records Schedule and the Date the file plan was created.


US Census Bureau **(OFFICE NAME) File Plan**

Types of Records	Disposition Instructions	Record Schedule
Types of Files	Disposition Instruction	Disposition Authority
EXAMPLES		
Subject Files	Destroy when no longer needed	GRS 23, item 7
Forms - BC-75/ BC-103/ CD 50s	TEMP - Destroy after 6 years	GRS 4.1, item 020
Procurement Files/ Contracts/ Paying Bills/ Invoices	TEMP - Destroy after 6 years	GRS 1.1, item 010

Page 18

Filing Records

- Let's take a look at the Census Office File Plan template. Mandatory entries in the file plan are Office Name, Type of Record, Disposition Instructions, Records Schedule and the Date the file plan was created.



Records Disposition


Disposition refers to actions taken with regard to Federal records that are no longer needed for current government business as determined by their appraisal pursuant to legislation, regulation, or administrative procedure. Disposition is a comprehensive term that includes both destruction and transfer of Federal records to the National Archives of the United States. For more detailed discussions of disposition and disposition programs, refer to 36 CFR Part 1226 or the [Disposition of Federal Records Handbook](#).

- **Temporary records** are those records that NARA approves for either immediate disposal or for disposal after a specified time or event.
- **Permanent records** are those that NARA appraises as having sufficient value to warrant continued preservation by the Federal Government as part of the National Archives of the United States

Page 19

Records Disposition

- Disposition refers to actions taken with regard to Federal records that are no longer needed for current government business as determined by their appraisal pursuant to legislation, regulation, or administrative procedure. Disposition is a comprehensive term that includes both destruction and transfer of Federal records to the National Archives of the United States. For more detailed discussions of disposition and disposition programs, refer to 36 CFR Part 1226 or the [Disposition of Federal Records Handbook](#). (make hyperlink)
- **Temporary records** are those records that NARA approves for either immediate disposal or for disposal after a specified time or event.
- **Permanent records** are those that NARA appraises as having sufficient value to warrant continued preservation by the Federal Government as part of the National Archives of the United States




One Method of Destruction

Census Headquarters is currently using one method of disposal for floors 2 through 8.

Why is this change being made?

- To prevent and avoid potential unauthorized sensitive material disposal
- Improved control over the destruction of sensitive materials
- Compliance with Census Bureau security policies, laws, and authorities approved by the Internal Revenue Service
- Improved business performance: Operating more efficiently and reducing cost
- Environmental protection: Reducing and mitigating environmental risks and pollution enables an organization to reduce its environmental impact and increase its operating efficiency



Floors 2-8

Page 20


One Method of Destruction

- Census Headquarters is currently using one method of disposal for floors 2 through 8.
- Why is this change being made?
- To prevent and avoid potential unauthorized sensitive material disposal
- Improved control over the destruction of sensitive materials
- Compliance with Census Bureau security policies, laws, and authorities approved by the Internal Revenue Service
- Improved business performance: Operating more efficiently and reducing cost
- Environmental protection: Reducing and mitigating environmental risks and pollution enables an organization to reduce its environmental impact and increase its operating efficiency

Title 26 – Federal Tax Information (FTI)

Title 26, Federal Tax Information (FTI), consists of confidential Census data. To dispose of FTI records:

- Record materials in the approved FTI Log, on page 22.
- Deposit records in blue locked bins marked **T26/FTI**; or
- Shred records using shredders that meet Census Bureau policy and are approved by the Census Bureau Office of Security.



page)

(change bullet 1 to say next

Title 26 - Federal Tax Information (FTI)

- Title 26, Federal Tax Information (FTI), consists of confidential Census data. To dispose of FTI records:
- Record materials in the approved FTI Log, on page 22.
- Deposit records in blue locked bins marked **T26/FTI**; or
- Shred records using shredders that meet Census Bureau policy and are approved by the Census Bureau Office of Security.

Documentation
FTI Log

ONLY LOG Title 26 Data/FTI


Year: _____ Secure Bin/Shredder Location: _____

Date	Division	Your Name (Printed)	Detailed Document Description	Confirm Doc is FTI	# of Pages	# of Copies	Select Disposal Method	
							Shred	Bin #

Page 22

Documentation FTI Log

- Only Log Title 26 Data/FTI



Printing & Disposition of FTI

Printing and/or disposal of FTI is permitted at both Census Bureau Headquarters and the National Processing Center (NPC).

At the Census Bureau HQ, printing and disposition are permitted in all locations **EXCEPT** for:

- 1st floor

At the NPC, all bins and printers have been approved for printing and disposition of FTI.

Page 23


Printing & Disposition of FTI

- Printing and/or disposal of FTI is permitted at both Census Bureau Headquarters and the National Processing Center (NPC).
- At the Census Bureau HQ, printing and disposition are permitted in all locations **EXCEPT** for the 1st floor
 - At the NPC, all bins and printers have been approved for printing and disposition of FTI.

Departing Personnel

Before a records management point of contact (POC) leaves the Agency:

- Designate a new POC and transition records to the new POC.
- Ensure records are identified and organized.
- Ensure the new POC can access all electronic records (email, password protected or encrypted files).
- Ensure the departing employee does not remove, delete or destroy any records.



Page 24

Departing Personnel

- Before a records management point of contact (POC) leaves the Agency:
- Designate a new POC and transition records to the new POC.
- Ensure records are identified and organized.
- Ensure the new POC can access all electronic records (email, password protected or encrypted files).
- Ensure the departing employee does not remove, delete or destroy any records.

**Unauthorized
Destruction/Mishandling
of Records**

Title 18, U.S.C. § 2071 lists the penalties for the unauthorized destruction or other mishandling of records.

Willful and unlawful concealment, removal, obliteration, destruction, mutilation, and/or falsification of Federal records can result in a fine or imprisonment not more than three years, or both.



Page 25


Unauthorized Destruction/Mishandling of Records

- Title 18, U.S.C. § 2071 lists the penalties for the unauthorized destruction or other mishandling of records.
- Willful and unlawful concealment, removal, obliteration, destruction, mutilation, and/or falsification of Federal records can result in a fine or imprisonment not more than three years, or both.

Records Management Summary

You've reached the end of the course. Remember:

- Records management is the law.
- Federal Records are:
 - Recorded information, regardless of form or characteristics, and
 - Evidence of organization, functions, policies, decisions, procedures, operations, or other activities.
- Everyone is responsible for managing records.
- PPM Chapter K-3, *Records Management*, states the Census Bureau's records management policy.



Page 26

Management Summary Records

You've reached the end of the course. Remember:

- Records management is the law.
- Federal Records are:

Recorded information, regardless of form or characteristics, and

- Evidence of organization, functions, policies, decisions, procedures, operations, or other activities.
- Everyone is responsible for managing records.
- PPM Chapter K-3, **Records Management**, states the Census Bureau's records management policy.



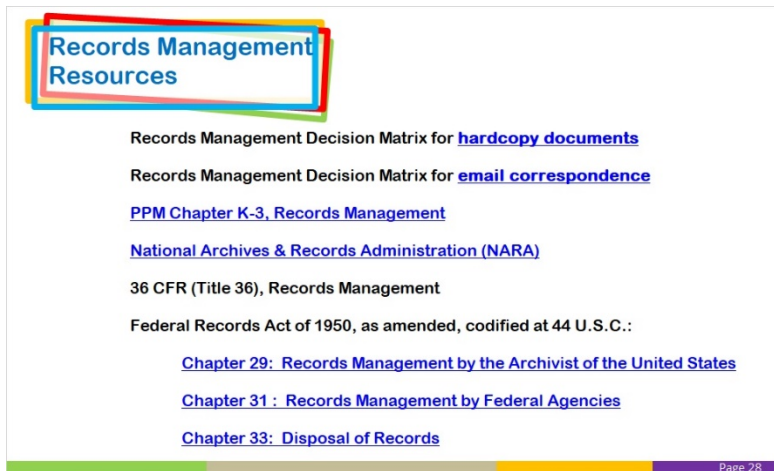
Records Management Summary (continued)

- The three stages to the life of Federal records are creation, maintenance/use, and disposition.
- Personal papers or files are not Federal records.
- Records are either temporary or permanent.
- The Census Bureau can destroy temporary records in accordance with records schedules.
- Permanent records warrant continued preservation as part of the U.S. National Archives.
- Title 18, U.S.C. § 2071 lists the penalties for the unauthorized destruction or other mishandling of Federal records.

Page 27

Records Management Summary (continued)

- The three stages to the life of Federal records are creation, maintenance/use, and disposition.
- Personal papers or files are not Federal records.
- Records are either temporary or permanent.
- The Census Bureau can destroy temporary records in accordance with records schedules.
- Permanent records warrant continued preservation as part of the U.S. National Archives.
- Title 18, U.S.C. § 2071 lists the penalties for the unauthorized destruction or other mishandling of Federal records.



Records Management Resources

Records Management Decision Matrix for [hardcopy documents](#)

Records Management Decision Matrix for [email correspondence](#)

[PPM Chapter K-3, Records Management](#)

[National Archives & Records Administration \(NARA\)](#)

36 CFR (Title 36), Records Management

Federal Records Act of 1950, as amended, codified at 44 U.S.C.:

[Chapter 29: Records Management by the Archivist of the United States](#)

[Chapter 31 : Records Management by Federal Agencies](#)

[Chapter 33: Disposal of Records](#)

Page 28

Records Management Resources

Records Management Decision Matrix for [hardcopy documents](#)

Records Management Decision Matrix for [email correspondence](#)

[PPM Chapter K-3, Records Management](#)

[National Archives & Records Administration \(NARA\)](#)


36 CFR (Title 36), Records Management

Federal Records Act of 1950, as amended, codified at 44 U.S.C.:


[Chapter 29: Records Management by the Archivist of the United States](#)

[Chapter 31 : Records Management by Federal Agencies](#)

[Chapter 33: Disposal of Records](#)



Need Assistance



Protect And Preserve
Records Management Office

The ACSD Records Management Office offers records analysis, audit and inventorying services. The team manages the Bureau's records storage, retrieval and disposition activities, and coordinates with NARA to develop and implement records schedules.

For help with managing office records, call the Records Management Team at (301) 763-2282, or visit the intranet [website](#) for more information.

TTY callers, contact the Federal Relay Service at 1-800-877-8339 and give them the number you would like to call.

Page 29

Need Assistance

The ACSD Records Management Office offers records analysis, audit and inventorying services. The team manages the Bureau's records storage, retrieval and disposition activities, and coordinates with NARA to develop and implement records schedules.

For help with managing office records, call the Records Management Team at (301) 763-2282, or visit the intranet [website](#) for more information.

TTY callers, contact the Federal Relay Service at 1-800-877-8339 and give them the number you would like to call.

Knowledge Checks**Question 1****What manual contains the Census Bureau Records Management Policy?**

Answer: PPM, Chapter K-1

PPM, Chapter K-2

PPM, Chapter K-3 (Correct Answer)

Question 2**At the Census Bureau, only Federal employees are responsible for managing records.**

Answer: False (Correct Answer)

True

Question 3**Which of the following is/are required of all Census personnel?**

Answer:

- Safeguard information that requires protections
- Manage records in accordance with approved records schedules
- Manage information that documents work performed
- All of the above (Correct Answer)

Question 4

At _____, printing and disposition are permitted in all locations **EXCEPT** for 1st Floor at _____, all bins and printers have been approved for printing and disposition of FTI.

Answer:

Field Division, Headquarters

Headquarters, National Processing Center (Correct Answer)

National Processing Center, Regional Office

Question 5**To properly care for Federal records:****(Select all that apply)**

Answer:

- Limit unnecessary copies (Correct Answer)
- Separate records from non-records (Correct Answer)
- Organize records in a protective manner (Correct Answer)

- Follow policies for storing, signing out, and using records (Correct Answer)

Question 6

A file inventory lists all records maintained by an office.

Answer:

- True (Correct Answer)
- False

Question 7

Mandatory entries in the office file plan include:

Answer:

- Arrangement
- Inclusive date (Correct Answer)
- Inventory creation date (Correct Answer)
- Disposition instructions (Correct Answer)

Question 8

The two types of records schedules are Federal Records Schedules and Census Bureau Records Schedule.

Answer:

- False (Correct Answer)
- True

Question 9

Unauthorized destruction or other mishandling of records could result in a fine, imprisonment of not more than three (3) years, or both

Answer:

- True (Correct Answer)
- False

Question 10

Records disposition is the action taken to dispose of records no longer needed for current government business.

Answer:

- True (Correct Answer)
- False



You have completed **Records Management Training For Census Employees & Contractors**.

Click the **EXIT COURSE** button below to close this course and complete the required end-of-course evaluation.

***Please allow 3-5 business days for course completion to be reflected in the CHRIS.**

[Exit Course](#)



You have completed **Records Management Training For Census Employees & Contractors**.

Certificate of Completion

(Name)

*successfully completed the
U.S. Census Bureau*

Census Bureau Records Management Training
on

(Date)

To obtain credit for completing this training, provide the following information and email it to:
acsd.records@census.gov

Your Information:

- **Name (printed)** _____
- **Signature** _____
- **Affiliation** _____
- **Division Name** _____

US Census Bureau

(OFFICE NAME) File Plan

Types of Records	Disposition Instructions	Record Schedule
Types of Files	Disposition Instruction	Disposition Authority
EXAMPLES		
Subject Files	Destroy when no longer needed	GRS 23, item 7
Forms - BC-75/ BC-103/ CD 50s	TEMP - Destroy after 6 years	GRS 4.1, item 020
Procurement Files/ Contracts/ Paying Bills/ Invocies	TEMP - Destroy after 6 years	GRS 1.1, item 010

Series Title	Series Description	Series Location	Inclusive Date	Media Type	Arrangement
Name of the File	Short description of the Record	Exactly where the record is located	Date range of the Record	Types of Record	How the Record is filed
EXAMPLES					
Time and Attendance	Records of Payroll/ Leave Requests / Sign in Sheets and records pertaining to time and attendance of employee	File Cabinet 4 outside 3J234	1/2015 to date	Paper	Alphabetically
Office Files	Routine Administrative Office Files	File Cabinet 2 outside 3J234	1/2010 to date	Paper	Alphabetically by subject
Training Materials	Training Manuals, Instructions and Quick Reference Materials	File Cabinet 5-8 outside 3J233	1/2014 to date	Paper	Alphabetically by subject
Form CD 50's	Personal Property Control Forms - Identify Bureau's property.	File Cabinet 2 outside 3J234	1/2014 to date	Paper	By Division

Appendix D: Data Stewardship and Information Technology Security Awareness Training and No Fear Act Training

This is a transcript of the Census Bureau's 2020 Data Stewardship and Information Technology (IT) Awareness training. You may print this transcript for future reference. If you have a disability and need reasonable accommodations to access this e-Learning course, please contact the Policy Coordination Office at 301-763-6440. If you have questions concerning any other accommodations, please contact the [Disability Program staff](#) at HRD.Accommodations@census.gov or 301-763-4060 (Voice). HRD's Information Technology Educational Services Branch is committed to providing access to our e-Learning courses for individuals with disabilities.

Section 508 requires that Federal agencies' electronic and information technology is accessible to people with disabilities. Additional information can be found at:

https://collab.ecm.census.gov/div/asd/intranet/Internet_Dissemination_Handbook/Pages/Policy_Section508.aspx .

You must also complete additional Title 26 Training if you work at:

- Census Bureau Headquarters
- National Processing Center (NPC)
- Bowie Computer Center
- Federal Statistical Research Data Centers
- Any other Census Bureau location where Title 26 information is stored or accessed

Contact your supervisor, Sponsor, or Contracting Officer's Representative (COR) COR for instructions.

Field Representatives (FRs), Enumerators, and Regional Staff (RO) staff generally do NOT need additional Title 26 training.

Course Introduction

Course Introduction, Screen 1

Screen Title:

2020 Data Stewardship and Information Technology Security Awareness Training

Screen Content:

Learn to:

- Protect the sensitive data we handle at the Census Bureau, as well as your own personal information.
- Recognize cyber-attacks and security incidents and what to do if they occur

We'll cover:

- Data Stewardship fundamentals
- Data Protection and the Law
- Safeguarding Data
- IT Security Threats, Vulnerabilities, and Countermeasures

Narration:

Welcome to the U.S. Census Bureau's Data Stewardship and Information Technology (IT) Security Awareness training. In this training, you'll learn how to protect the sensitive data we handle at the Census Bureau, as well as your own personal information. You will also learn how to recognize cyber-attacks and information security incidents, and what you should do if they occur.

We'll cover the fundamentals of the Census Bureau's Data Stewardship program; the laws that require us to protect data at the Census Bureau; the tools and methods we use to safeguard data; and IT security threats, vulnerabilities, and countermeasures.

Plan to spend about sixty minutes to complete this training. This course contains three modules and one knowledge check. To receive credit for completing this course, you must receive a score of 70% or higher. Let's get started.

Module 1

Module 1, Screen 2:

Screen Title:

Data Stewardship Fundamentals

Screen Content:

Learning Objectives:

- Data Stewardship Defined
- Data Protection and the Law
- Types of Data at the Census Bureau
- Fundamental Behaviors that Protect Data

Narration:

In this section, you will learn about what Data Stewardship is and why it is important, the laws that protect data, the types of Census Bureau data and the laws that protect them, and the fundamental responsibilities that protect data.

Module 1, Screen 3:

Screen Title:

Data Stewardship Defined

Screen Content:

The formal and continuous process we use to care for the information that is entrusted to us. Why is data stewardship so important?

- It's vital for the public trust
- It's required by law
- It protects individuals
- It creates a secure network
- You are the most important part of Data Stewardship

Narration:

Data Stewardship is the formal and continuous process we use to care for the information that is entrusted to us. This can be information we collect, receive, or release, as well as information about our employees.

We rely on individuals and organizations to provide us with their information. They are willing to do this because they trust that we will keep their information confidential. Gaining and keeping public trust allows us to collect the information we need to do our jobs.

One of the most important reasons to practice good Data Stewardship is simple: The law requires it.

By practicing good Data Stewardship, we protect individuals from identity theft and the release of their personal information.

We depend on a secure network to safely house the personal information of millions of Americans. By being aware of threats to our network, you can help keep it safe and secure.

Without a secure network, information could fall into the wrong hands.

You are responsible for following the laws, regulations, and policies that protect information.

Module 1, Screen 4:

Screen Title:

Privacy Principles

Screen Content:

The backbone of Data Stewardship

- They are the ethical guidelines that ensure we protect the public's personal information.
- Each privacy principle represents a promise

It's important for all Census Bureau employees to understand the Privacy Principles

Narration:

The backbone of data stewardship is the Census Bureau's Privacy Principles. These ethical guidelines help ensure we protect the public's personal information throughout all of our activities. Each privacy principle represents a promise to our respondents, employees, and the American Public.

Under necessity,

- We promise to only collect information necessary for each survey or census.
- We promise to only collect the information we need to produce statistics about the population and economy of the United States.

Under Openness,

- We promise to let the public know why we are conducting the survey or census, why we are asking specific questions, and how their information will be used.

Under respectful treatment,

- We promise to collect data in a way that minimizes respondents' time and effort.
- We promise to only engage in legal, ethical, and professionally accepted data collection practices.

Under confidentiality,

- We promise that every person with access to sensitive information is sworn for life to protect it. And,
- We promise that we will use up-to-date technology, statistical methodology, and physical security procedures to protect their information.

Module 1, Screen 5:

Screen Title:

Privacy Versus Confidentiality

Screen Content:

- Privacy is respecting individuals' freedom from unauthorized and unwarranted intrusion into their personal information.
- Confidentiality is protecting sensitive information we've collected from unauthorized disclosure
- Privacy: What data we collect.
- Confidentiality: How we protect data.

Narration:

Privacy and confidentiality are terms that are often used interchangeably, but there is a difference between the two.

Privacy is respecting individuals' freedom from unauthorized and unwarranted intrusion into their personal information, being transparent about the data collected (including its purposes and disclosures, etc.), and allowing corrections of personal data we have on record that are inaccurate, incomplete, untimely, or irrelevant. Confidentiality is protecting sensitive information from unauthorized disclosure after we've collected it.

Module 1, Screen 6:

Screen Title:

Oath of Non-Disclosure

Screen Content:

You Started with an Oath

- Our employees take the oath because we depend on the public's cooperation and trust
- We promise to protect the personal information they provide

Narration:

You promised to adhere to laws protecting data when you started with the Census Bureau and took the Oath of Non-disclosure. When you took the oath of non-disclosure, you joined a group of committed individuals sworn for life to protect information.

Our employees take the oath of non-disclosure because we depend on the public's cooperation and trust and we promise to protect the personal information they give us.

Module 1, Screen 7:

Screen Title:

Data Protection and the Law

Screen Content:

Laws and regulations control what information we collect and how we collect it, keep it safe, and release it.

Anyone who handles sensitive information is personally responsible for following these laws and regulations

Allowing unauthorized access to protected information, even if by accident, is against the law.

Some sensitive information is protected by more than one law

Key Laws:

- Title 13 U.S.C.: The Census Act
- Title 26 U.S.C.: The Internal Revenue Code
- Title 5 U.S.C.: Includes the Privacy Act of 1974

Narration:

The laws you swore to uphold guide everything we do at the Census Bureau.

Anyone who handles sensitive information is personally responsible for following these laws and regulations.

Allowing unauthorized access to protected information, even if by accident, is called unauthorized disclosure and is against the law. The penalties can be severe.

The key laws that govern data stewardship at the Census Bureau are:

- Title 13 U.S.C.: The Census Act
- Title 26 U.S.C.: The Internal Revenue Code
- Title 5 U.S.C.: Including the Privacy Act of 1974

It's also important to know that some sensitive information is protected by more than one law.

Module 1, Screen 8:

Screen Title:

Title 13 U.S.C.: The Census Act

Screen Content:

An image of a paper survey and pen are displayed.

- Authorization
- Confidentiality
- Protections:
 - Respondent information is never published.
 - We collect information only to produce statistics and cannot be used against individuals by any government agency or court.
 - You are sworn for life to protect confidentiality

Violating the law is a felony and includes penalties of a federal prison sentence of up to 5 years, a fine of up to \$250,000 dollars, or both.

The Confidential Information Protection and Statistical Efficiency Act (CIPSEA)

NOTE: When the Census Bureau conducts surveys for other agencies the data may be protected under the Confidentiality Information Protection and Statistical Efficiency Act (CIPSEA). We protect any data we collect under CIPSEA just like data collected under Title 13.

Narration:

Title 13 is the federal law that authorizes and directs the Census Bureau to conduct censuses, surveys, and other statistical work; and sets the standards of confidentiality for our data. The law requires the Census Bureau to keep respondent information confidential and only use it for statistical research.

It is against the law to disclose or publish any respondent data, sampling or address information, or administrative data collected under Title 13.

The information we collect is only for producing statistics and cannot be used against individuals by any government agency or court.

All Census Bureau employees and the Special Sworn Status individuals who assist us with our work are sworn for life to protect respondent confidentiality even after leaving the Census Bureau.

Violation of this law carries severe penalties, including a federal prison sentence of up to five years, a fine of up to \$250,000, or both.

NOTE: The Census Bureau also conducts surveys for other agencies. Typically, these data are also protected by Title 13, however in some cases, the confidentiality of the data are protected by the

sponsoring agency's laws. The most common of these laws is the Confidential Information Protection and Statistical Efficiency Act (also known as CIPSEA). We use the same safeguards to protect data we collect under CIPSEA as we use for data collected under Title 13.

Module 1, Screen 9:

Screen Title:

Title 26 U.S.C.: The Internal Revenue Code

Screen Content:

Authorizes the Internal Revenue Service (IRS) to share Federal Tax Information (FTI) with the Census Bureau for statistical purposes only

Penalties include:

- Fines of up to \$600,000,
- A prison sentence of up to 22 years,
- Or both

Comingled Data

- Title 26 protected data mixed with Title 13 protected data
- Unauthorized disclosure of comingled data is subject to penalties of BOTH laws

NOTE: You may be required to take a separate training on Title 26 requirements. Contact your supervisor, sponsor, or Contracting Officer's Representatives (COR) for more information.

Narration:

The Internal Revenue Service is authorized by law to share Federal Tax Information (also known as FTI) with the Census Bureau for statistical purposes only.

Violating Title 26 is a felony and carries severe penalties including fines of up to \$600,000, a prison sentence of up to 22 years, or both.

Please be aware that if data protected under Title 26 is mixed in any way with data protected under Title 13, it is comingled data. Anyone responsible for the unauthorized disclosure of comingled data is subject to the combined penalties of BOTH laws.

NOTE: If you work at Census Bureau Headquarters, most other Census Bureau buildings, or work with or around FTI, you are required to take a separate training on Title 26 requirements. Contact your supervisor, sponsor, or COR for more information.

Module 1, Screen 10:

Screen Title:

Title 5 U.S.C. 552a; Includes the Privacy Act of 1974

Screen Content:

Title 5 protects Personal information, including yours.

- Protects records of individuals
- Protects respondent, vendor and personnel information

Privacy Act System of Records (SOR)

- A group of more than one record containing information about individuals
- Retrieved by name or other personal identifier

System of Records Notice (SORN)

- Public notice published in the Federal Register describing a SOR is called a SORN

Narration:

Title 5; The Privacy Act of 1974 protects personal information (including yours) from unauthorized disclosure.

The Privacy Act of 1974 protects personal information collected by the federal government and stored in a system of records. For the Census Bureau this includes respondent, vendor and personnel information.

The Act defines a System of Records as more than one record containing information about individuals where the information is retrievable by name or other personal identifier.

It also requires that federal agencies publish a System of Records Notice in the Federal Register any time they create or change a System of Records.

Module 1, Screen 11:

Screen Title:

Other Policies that Protect Data

Screen Content:

Census Bureau Policies are also shaped by:

- Department of Commerce
- Conduct Privacy Impact Assessments (PIAs) before developing, obtaining, or revising IT

systems Office of Management and Budget (OMB)

- National Institute for Standards and Technology (NIST)

DS-007, Safeguarding and Managing Information:

- Defines roles and responsibilities of individuals who have access to our data
- Establishes the guidelines for how we handle data at the Census Bureau

Narration:

In addition to the laws discussed, policies issued from the Department of Commerce and other agencies, such as OMB and NIST, help structure the Census Bureau policies that govern how we handle data, produce and disseminate our statistical products, and secure our information systems.

For example, the Census Bureau Safeguarding and Managing Information policy (or DS-007) is based on NIST guidelines and defines the roles and responsibilities of individuals who have access to our data.

This policy also establishes the data handling guidelines for the Census Bureau.

You'll learn more about how this and other policies help you protect data later in the training.

Module 1, Screen 12:

Screen Title:

Types of Data at the Census Bureau

Screen Content:

Click to learn more and see examples of each (types of data):

- Personally Identifiable Information (PII)
- Business Identifiable Information (BII)
- Title 13 Protected Data
- Title 26 Protected Data
- Administratively Restricted
- Public Use

Narration:

One of the most important things you can do as a good data steward is learn to recognize the type of data you're working with so you can handle and safeguard it appropriately.

Click the buttons to learn more and see examples of each.

When in doubt, contact your supervisor for guidance.

Module 1, Screen 12.1:

Screen Title:

Personally Identifiable Information (PII)

Screen Content:

Sensitive on Its Own

- Social Security Number
- Financial account numbers
 - credit card
 - bank account numbers
- Medical Information
- Results of background investigations
- Disciplinary action history

Sensitive When Combined

- Name + date or place of birth
- Performance plan + ratings

Narration:

Information about people is called Personally Identifiable Information, or PII. We get PII from surveys, administrative records, and you, our employees.

When people think of PII they usually think of things such as names, birth dates, addresses, phone numbers etc. Some PII, such as your name, by itself, isn't sensitive because while it identifies you as an individual, it won't cause you any harm if released. However, it's important to know that some PII is sensitive, and sometimes PII becomes more sensitive depending on what it is combined with. These data, if released can cause harm to individuals.

Some PII is only sensitive when combined, for example:

- Name + date or place of birth
- Performance plan + ratings

These examples do not cover everything. There may be other information that could be used to identify individuals.

Module 1, Screen 12.2:

Screen Title:

Business Identifiable Information (BII)

Screen Content:

- Business name
- Address
- NAICS code
- Number of employees
- Payroll
- Sales
- Assets
- Financial data

Narration:

We get Business Identifiable Information or BII from surveys, administrative records, contracts, agreements, and other sources.

The examples you see on the screen do not cover everything. There may be other information that could be used to identify businesses and other organizations.

Module 1, Screen 12.3:

Screen Title:

Title 13 Protected Data

Screen Content:

- Business name
- Address

Data protected by Title 13 Includes:

- All Respondent PII and BII
 - **All** individual census or survey responses
 - Respondent contact information
- Address lists and frames including the Master Address File (MAF).
- Administrative records from other agencies and other third-party data acquired by the Census Bureau

Requires Disclosure Review Board (DRB) Approval

- Microdata
- Aggregate statistical information

Paradata Protected by Title 13 includes:

- Internet Paradata

- Contact History Instrument (CHI)
- Method of Interview
- Time and Date Stamps
- Keystroke data
- Audit trail and trace files
- Information on Primary Sampling Units (PSU) workloads
- Non-response, refusals, and don't know responses
- Notes on a case observations made by field representatives

[<Link to the Collection and Use of Paradata available to internal users only>](#)

Narration:

Most of the data that the Census Bureau collects, even for our reimbursable surveys and administrative data projects, is protected by Title 13. Title 13 doesn't just protect respondent PII and BII, this information handling category also includes all of the examples on the screen. Title 13 also protects information about an individual or household's participation or completion status, or their behavior during a data collection, which is commonly referred to as paradata. Click the link to learn more about the collection and use of paradata.

Module 1, Screen 12.4:

Screen Title:

Title 26 Protected Data

Screen Content:

Federal Tax Information (FTI) examples include:

- 1040 IRS Individual Tax Returns,
- 1099 IRS Information Returns,
- 1099-R (subset of information returns),
- Some Social Security Administration data
 - Master Earnings File
- Fact of Filing

Comingled Data

- Economic Census Files
- Quarterly Financial Report
- Business Register

Narration:

We receive Title 26 protected FTI from the IRS and use it in many of our statistical programs. Examples include:

- 1040s
- 1099s
- 1099-Rs
- some Social Security Administration data such as the Master Earnings File
- and any information that discloses Fact of Filing

Comingled Data is Title 13 data linked to FTI and includes examples such as:

- Economic Census Files,
- Quarterly Financial Report,
- and the Business Register

Module 1, Screen 12.5:

Screen Title:

Administratively Restricted Data

Screen Content:

Examples include:

- For Official Use Only or Internal Use only documents and files
- Pre-decisional documents or drafts
- Contracting information
- Financial information
- Security documents
- Embargoed data or reports that have not been released but meet Disclosure Review Board (DRB) requirements for public release.
- Internal use methodological documentation
- Pre-release Principal Economic Indicators and Demographic Time-Sensitive Data.
- Agreements with other entities such as Interagency Agreements

Narration:

Information about internal operations is considered Administratively Restricted

Administratively restricted information includes:

- For Official Use Only information

- Pre-decisional documents or drafts
- Internal Census Bureau documentation such as contracting documents
- Reports that meet Disclosure Review Board requirements, but are not yet cleared for release such as embargoed data.
- There may be other information not protected by statutory authority, but still subject to access restrictions.

Module 1, Screen 12.6:

Screen Title:

Public Use

Screen Content:

- Published Statistical products
- Statistical products, papers, reports, that meet the statistical quality standards and have been approved by the Disclosure Review Board
- Information released through the Freedom of Information Act Office (FOIA)
- Promotional products
- Smartphone Apps
- News Releases
- Videos & Radio features
- Data visualizations
- Content on www.census.gov

Narration:

We review everything we release to the public to make sure it doesn't disclose any sensitive information and meets our quality standards. Please see the screen for examples.

Module 1, Screen 13:

Screen Title:

Your Responsibilities

Screen Content:

Your Responsibilities

Avoiding and Reporting Security Incidents

- Following the Data Handling Guidelines, IT Acceptable Use Policy, and other Census

Bureau policies

- Report confirmed or suspected incidents to the Census Bureau Computer Incident Response Team (BOC CIRT) within one hour

Unauthorized Browsing

- Do not look through any Sensitive PII or BII, Title 13, Title 26 or administratively restricted information without a work-related need
- Penalty is disciplinary action up to and including termination of employment

Personal Use and Gain

- We follow the Census Bureau ethical guidelines and never use Census Bureau information for personal use or benefit
- Violating these ethical guidelines carries harsh penalties including termination of employment and legal consequences

Complete Annual Trainings

One of the best practices to be good data stewards is to stay compliant with annual mandatory trainings including:

- This training: Data Stewardship and IT Security Awareness Training
- And Title 26 Training

Your network access will be terminated if you fail to complete annual trainings

Narration:

You are personally responsible for following the Data Handling Guidelines, IT Acceptable Use Policy and other Census Bureau policies that help us avoid information security incidents.

You are also responsible for reporting any confirmed or suspected IT security incidents or any mishandling of Title 5, Title 13, Title 26, or administratively restricted information to the Census Bureau Computer Incident Response Team (BOC CIRT) within one hour.

These policies and how to report an incident are discussed later in the course.

Unauthorized Browsing

- Do not look through any sensitive PII or BII, Title 13, Title 26 or administratively restricted information that you do not have a work-related need to access. This is strictly prohibited and can result in disciplinary action up to and including termination of employment.

Personal Use and Gain

- We follow the Census Bureau ethical guidelines and never use Census Bureau information

for personal use or benefit.

- Violating these ethical guidelines carries harsh penalties including termination of employment and legal consequences.

Complete Annual Trainings

You must stay compliant with annual mandatory trainings which includes taking:

- This training, the Data Stewardship and IT Security Awareness Training which must be completed by all Census Bureau employees, all contractors, and all those who have Special Sworn Status (SSS) and access to the Census Bureau network.
- And Title 26 Training if you work at:
 - Census Bureau Headquarters
 - The National Processing Center (NPC)
 - The Bowie Computer Center
 - Any Federal Statistical Research Data Center
 - Any other Census Bureau locations where FTI are stored, processed, or handled.

Your network access will be terminated if you fail to complete annual trainings

Module 2

Module 2, Screen 14:

Screen Title:

Safeguarding Data

Screen Content:

Learning Objectives

In this module you will learn about the Census Bureau safeguard procedures for:

- Printing and managing hardcopies
- Electronic transmission of data
- Data labeling
- Reviewing and approving data prior to release
- Physically safeguarding data
- Safely working in alternate work places
- Identifying and reporting information security incidents

Narration:

You've learned about the importance of data stewardship as well as the laws, policies, and behaviors that protect Census Bureau data. You have also learned about the different types of Census Bureau data and how to recognize them.

In this module, you will learn the procedures for safeguarding and handling Census Bureau data and how to identify and report an information security incident.

Module 2, Screen 15:

Screen Title:

Frequently Asked Data Handling Questions

Screen Content:

A link to the Census Bureau Data Handling Guidelines, Appendix A of this document.

Narration:

In your day-to-day work you will always want to be sure that you are handling information appropriately. If you have questions, it is always a good idea to check with your supervisor.

Let's go over some of the most common questions people ask about how to handle data and other information.

For more information, click the link for the Census Bureau Data Handling Guidelines (this is Appendix A)

Module 2, Screen 16:

Screen Title:

Printing and Managing Hardcopies

Screen Content:

Printing and Managing Hardcopies

What needs to be printed with a cover page or with private printing?

- Sensitive PII
- Title 13
- Title 26

What needs to be logged when printing?

- Title 26

What types of data need to be locked away when not in use?

- Sensitive PII
- Title 13
- Title 26
 - Cabinets or other storage devices holding Title 26 data must be labeled appropriately.
- High sensitivity Administratively Restricted information
 - Ask you supervisor when you are not sure about the sensitivity

Can I take hard copies of my work home with me when I telework?

- Depends on the type of information
- NEVER remove hard copies of Title 13 or Title 26 protected data from secure Census Bureau facilities

How should I ship hard copies?

- Double Wrap
- Ship using an approved, traceable carrier.

Narration:

Printing and Managing Hardcopies

What needs to be printed with a cover page or with private printing?

Sensitive PII, Title 13, and Title 26 data must be printed with a cover page and must be immediately removed from the printer. We encourage you to use private printing for any documents containing these data if possible.

What needs to be logged when printing?

You must log any printouts of Title 26 data in the log book next to the printer that you use.

What types of data need to be locked away when not in use?

It is always important to lock away Sensitive PII, Title 13, or Title 26 in a desk or file cabinet when not in use. Never leave these printouts on your desk, in conference rooms, in the bins by the restrooms, or in any public space.

Any cabinets or other storage devices containing Title 26 data must be labeled appropriately. Refer to the Title 26 Awareness Training for guidance.

You must restrict access to hardcopies of these data to only Census Bureau staff, contractors, or other individuals with Special Sworn Status who have a business need to know.

In general, you should handle administratively restricted information based on its sensitivity. For example, pre-award contracting information should be locked away, but a draft presentation may not need to be. If you have any questions on handling these types of information, contact your supervisor.

Can I take hard copies of my work home with me when I telework?

It depends on the type of information that you work with. You must NEVER remove hard copies of Title 13 or Title 26 protected data from secure Census Bureau facilities, even for telework.

How should I ship hard copies?

In general, if shipping hard copy Sensitive PII, Title 13, or Title 26, you must double wrap and ship using only an approved, traceable carrier.

Module 2, Screen 17:

Screen Title:

Electronic Data Transmission

Screen Content:

Electronic Transmission of Data

When do I need to encrypt my email?

Encrypt when email contains:

- Sensitive PII
- Title 13
- Title 26
- High sensitive Administratively Restricted information

How do I encrypt electronic transmissions?

- Do not put sensitive information in the body of the email, you must send as an attachment.
- Use approved encryption tools such as Department of Commerce Kiteworks software

What data can I telework with?

- Census Bureau employees can telework with Title 13 and Title 26 data only through Virtual Desktop Infrastructure (VDI) or Virtual Private Network connection if using a Census-issued laptop.
- Contractors and Special Sworn Status (SSS) are NOT authorized to work remotely with Title 26 data.
- Never email yourself Title 13 or Title 26 data for use on your personal computer.

Can I share data while videoconferencing?

- Sensitive PII and Title 13 data is authorized for video conferencing ONLY using Census Skype for Business.
- Title 26 data is NOT authorized for use in any videoconferencing applications.

< Link to Skype for Business with Title 13 and Sensitive PII Guidance available for internal users only>

Can I fax data?

- Yes, with some cautions. If faxing sensitive information, ensure someone is at the machine to receive it and confirm receipt after sending.

Narration:

Electronic Transmission of Data

When do I need to encrypt my email?

You must always encrypt an email or other electronic transmission when the transmission contains Sensitive PII, Title 13 data, or Title 26 data. You must encrypt Administratively Restricted information when the sensitivity is high. Check with your supervisor about the sensitivity of the information if needed.

How do I encrypt electronic transmissions?

Never put sensitive information in the body of an email, instead you must send as an encrypted attachment. Use encryption tools such as Department of Commerce Kiteworks software. If you have questions about encrypting information, ask your supervisor.

What data can I telework with?

When teleworking, only access Title 13 and Title 26 data through the Virtual Desktop Infrastructure (VDI) or Virtual Private Network connection if using a Census-issued laptop. Never email yourself Title 13 or Title 26 data for use on your personal computer.

It is also important to note that contractors and Special Sworn Status (SSS) individuals are NOT authorized to work remotely with Title 26 data.

Can I share data while videoconferencing?

Sensitive PII and Title 13 data is authorized for video conferencing ONLY using Census Skype for Business. **Title 26 data is NOT authorized for use in any videoconferencing applications.** For more information about teleconferencing with Skype for Business, click the link for Skype for Business with Title 13 and Sensitive PII Guidance

Can I fax data?

Yes, you can with some cautions. If faxing sensitive information, ensure someone is at the machine to receive it and confirm receipt after sending. Contact the Policy Coordination Office for more information.

< Link to Skype for Business with Title 13 and Sensitive PII Guidance available to internal users only>

Module 2, Screen 18:

Screen Title:

Electronic and Hardcopy Data Labeling

Screen Content:

How should I label Title 13 data?

- Label “Disclosure Prohibited – Title 13 U.S.C.”

How should I label Title 26?

- Label “Disclosure Prohibited – Federal Tax Data Protected by Title 26 U.S.C.”

How should I label Administratively Restricted Information?

- Label examples include:
 - For Official Use Only.
 - For Internal Use
 - Pre-decisional

Narration:

Electronic Transmission of Data

How should I label Title 13 data?

- Label any documents (electronic or hardcopy) containing Title 13 data with “Disclosure Prohibited – Title 13 U.S.C.”

How should I label Title 26?

- Documents containing Federal Tax Information must be labeled “Disclosure Prohibited – Federal Tax Data Protected by Title 26 U.S.C.”

How should I label Administratively Restricted Information?

Label Administratively Restricted Information appropriately depending on what information the document contains and who the intended audience is. Some examples of appropriate labels are:

- For Official Use Only.
- For Internal Use
- Pre-decisional

If you have questions about labeling administratively restricted information, contact your supervisor.

Module 2, Screen 19:

Screen Title:

Disposal and Destruction

Screen Content:

What data must be disposed of in locked bins?

- Sensitive PII
- Title 13
- Title 26
- Administratively Restricted

Can I use a shredder?

- Yes, but only if the shredder is compliant with National Security Agency (NSA) high security performance requirements
- If you have questions, ask your supervisor

What data must be logged when disposed of or destroyed?

- Title 26

Narration:

Disposal and Destruction

What data must be disposed of in locked blue bins?

- Sensitive PII, Title 13, Title 26, and Administratively Restricted documents must be disposed of in the locked blue bins

Can I use a shredder?

- Some offices use shredders that must meet the performance requirements of the National Security Agency (NSA) and produce particles that are 1 x 5 millimeters in size. You may use these shredders to destroy hardcopies of sensitive information, if they are available. If you have questions, ask your supervisor.

What data must be logged when disposed of or destroyed?

- You must log the disposal of any Title 26 protected hardcopies in the disposal logs located

with the blue bins or compliant shredders.

Module 2, Screen 20:

Screen Title:

Data Review before Release

Screen Content:

- All information at the Census Bureau undergoes thorough review before it is publicly released.
- We review everything that is released to ensure that it is high quality and does not present a risk for disclosure.
- YOU safeguard information by being knowledgeable about and following the proper channels to have information released.
- Click the buttons on the screen for information about how different types of information is reviewed and released.
- If you have questions about what can be released to the public, contact your supervisor.

Buttons to pop-up slides:

- Survey Microdata, Tabulations, and Statistical Products
- Information Requests from the Public
- Information Requests from the Media
- Social Media

Narration:

All information at the Census Bureau undergoes thorough review before it is publicly released. We review everything that is released to ensure that it is high quality and does not present a risk for disclosure.

YOU safeguard information by being knowledgeable about and following the proper channels to have information released. Click the buttons on the screen for information about how different types of information is reviewed and released. If you have questions about what can be released to the public, contact your supervisor.

Module 2, Screen 20.1:

Screen Title:

Survey Microdata Tabulations and Statistical Products

Screen Content:

Disclosure Review Board

- The Disclosure Review Board (DRB) and Disclosure Avoidance Officers (DAOs) review and clear all Title 13 and Title 26 microdata, tabular data, and other statistical products prior to release
- For questions about Disclosure Review, contact your DAOs

Quality Review

Statistical Quality Standards

- All Census Bureau data publications must meet these internal quality standards

Public Information Office (PIO)

- Must be notified of materials being prepared for external distribution
- Subject matter division chiefs and associate directors are responsible for ensuring technical accuracy

Narration:

It is essential that we review all of our data products to ensure that they don't disclose any information protected by law. The Disclosure Review Board (DRB) and Disclosure Avoidance Officers (DAOs) review and clear all microdata, tabular data, and other statistical products prior to release. For questions about the Disclosure Review process, please visit the DRB's intranet site or contact your division's DAO. It is also critical that the Census Bureau produce high quality reliable data. All of our data publications must meet the Census Bureau's Statistical Quality Standards.

Public Information Office (PIO): The PIO must be notified of all appropriate materials (such as reports, new product updates, presentations, and datasets) being prepared for external distribution. Appropriate subject matter division chiefs and associate directors are responsible for ensuring the technical accuracy of information.

Module 2, Screen 20.2:

Screen Title:

Requests from the Public

Screen Content:

Freedom of Information Act (FOIA)

- Requests from the public must be routed through the Freedom of Information Act (FOIA) Office.
- The FOIA Office coordinates all releases under the FOIA and the Privacy Act.

- If a FOIA or Privacy Act request comes to you directly, do not answer it. Release of some information may require DRB review and approval.
- If the FOIA Office tasks you to provide records related to a request, send them as encrypted attachments or hand deliver in a sealed envelope.
- The Census Bureau's FOIA Officer officially determines what information can be released and redacts information not releasable. Do not black out information yourself. Release of some information may require DRB review and approval

Custom Tabulations

- You may answer general questions about products we release; however, you may not create and release custom tabulations upon request from the public unless authorized to do so.

[<Link to the Custom Tabulations and Extracts Policy for internal users only>](#)

Narration:

The Freedom of Information Act (FOIA) Office is responsible for coordinating any request for Census Bureau internal documents made by the public, or for any requests an individual may make for their personal records under the Privacy Act. If a FOIA or Privacy Act request comes to you directly, you must not answer it yourself. Instead contact the FOIA Office. If the FOIA Office tasks you to provide records related to a request, send them as encrypted attachments or hand deliver in a sealed envelope. The Census Bureau's FOIA Officer alone makes the determination of what information is exempted from disclosure. Do not black out any information yourself. Release of some information may require DRB review and approval. Contact your supervisor if you have questions about information requests.

Custom Tabulations

You may answer general questions about products or how to locate information we've already released, however you may NOT create and release custom tabulations or data extracts upon request from the public except as authorized by the Custom Tabulations and Extracts Policy. Click the link to learn more.

Module 2, Screen 20.3:

Screen Title:

Requests from the Media

Screen Content:

- The Census Bureau aims to make publicly available information accessible to the news media in a timely and accurate fashion.

- Consult the Public Information Office (PIO) if you receive requests from members of the media.
- Report news media and non-news media content provider contacts to the PIO before information is released.

For reporting media contacts, staff should:

- Use the Media Inquiry Form BC-1705 on PIO's intranet site,
- Email pio@census.gov,
- Or call 301-763-3030 within 24 hours of the media contact.

Narration:

The Census Bureau aims to make publicly available information accessible to the news media in a timely and accurate fashion. If you are contacted about requests for interviews, statements about data, or about results from members of the media, consult the PIO. All Census Bureau staff must report their news media and non-news media content provider contacts to the PIO before the information is released. See the screen for the PIO contact information.

Module 2, Screen 20.4:

Screen Title:

Social Media

Screen Content:

- Unless authorized, you are NOT permitted to post on social media sites in an official capacity as a Census Bureau employee
- Unless authorized, you may not sign up for social media accounts on behalf of the Census Bureau
- Authorized employees using social media in an official capacity must:
 - Use only on approved accounts
 - Only use official e-mail or other contact information for the creation and management of those accounts.
 - Never post sensitive information

<Link to the Department of Commerce Policy on the Approval and Use of Social Media and Web 2.0. This is Appendix B.>

Social Media and Respondents

- Never share respondent information or contact them directly through social media
- Do not contact respondents at their work place or work phone without permission

<Link to the Use of Public Websites to Obtain Respondent Contact Information Policy. This is Appendix C.>

Narration:

It's VERY important to know there are limitations to how you may use social media while working for the Census Bureau. You may not create social media accounts using your census.gov email address or on behalf of the Census Bureau. Unless authorized, you are NOT permitted to post on social media sites in your official capacity. You must also remember to confirm that all information shared through social media is approved, publically releasable information. Contact the Social Media Working Group for more information. Click the link to view the Department of Commerce Policy on the Approval and Use of Social Media and Web 2.0 (this is Appendix B)

Social Media and Respondents: It is important to remember that social media should not be used to interact directly with respondents.

- Never share respondent information or contact them directly through social media.
- Never contact a respondent at their work address or work phone number that they may have shared on social media unless they have given you permission.

Click the link for more information on the Use of Public Websites to Obtain Respondent Contact Information Policy (this is Appendix C).

Module 2, Screen 21:

Screen Title:

Physical Safeguards

Screen Content:

Physical security in the office can include:

- Badges for employees and contractors
- Temporary badges and escorts for visitors
- Building and elevator access limited to badge holders
- Fenced Perimeter and guarded gates
- Parking passes
- Locking work when not in use

Narration:

Physical safeguards ensure the safety of Census Bureau personnel, information, computer resources, facilities, and other assets.

Physical safeguards within Census Bureau facilities include:

- Badges for employees and contractors to gain entrance to the building and move around the building
- Temporary badges and escorts for visitors
- Building and elevator access limited to badge holders
- Fenced perimeter and guarded gates
- Parking passes

Individuals who work with Census Bureau data are the first line of defense, and one of the best ways of protecting data is locking work away when not in use.

Module 2, Screen 22:

Screen Title:

Lock it up!

Screen Content:

- Lock your computer when not in use by hitting control-alt-delete followed by the enter key
- Take your ID badge with you when you leave.
- Lock your Census Bureau issued devices when not in use. Don't leave them unattended.
- Do not share your Census Bureau issued device with other people
- Put sensitive data away and lock your desk when you leave your workstation.
- Lock your pod or office when you leave.
- Put any sensitive materials or devices in the trunk of your car, and lock your car if you're going to leave it unattended

Narration:

When it comes to protecting sensitive information at the Census Bureau, all of our IT and physical security measures revolve around a very basic concept: Restrict Access. What's the best way to restrict access to something? You lock it up!

- Lock your computer when not in use
- Take your ID badge with you when you leave your workstation.
- Lock your Census Bureau issued devices when not in use. Don't leave them unattended.
- Do not share your Census Bureau issued device with other people
- Put sensitive data away and lock your desk when you leave your workstation.
- Lock your pod or office when you leave.

- If working in the field, put any sensitive materials or devices in the trunk of your car, and lock your car if you're going to leave it unattended.

Module 2, Screen 23.1:

Screen Title:

Headquarters and all Census Bureau Building Badges

Screen Content:

- Always use your own badge credential to enter and exit Census Bureau buildings, elevators (going up and down), stairwells, and other secure spaces.
- Don't ask others to badge for you.
- Don't use your badge to allow others into the building, stairwells, elevators, or other secure spaces.

Remember:

- One person per badge-swipe (no piggybacking).
- Put any sensitive materials or devices in the trunk of your car, and lock your car if you're going to leave it unattended

Narration:

Restricting access also involves consistent badge use. Always use your own badge credential to enter and exit Census Bureau buildings, elevators (going up and down), stairwells, and other secure spaces.

Don't ask others to badge for you.

Don't use your badge to allow others into the building, stairwells, elevators, or other secure spaces unless you are escorting an individual wearing a visitor badge.

Remember: One person per badge-swipe (no piggybacking).

Module 2, Screen 23.2:

Screen Title:

Headquarters Badges

Screen Content:

Always scan badge in elevators or stairwells, even when going to the first floor of the building.

If you've left your badge at your desk, visit the security office in the Metro lobby, 1st floor, to get a temporary one.

Narration:

Always scan your badge in elevators or stairwells, even when going to the first floor of the building. If you've left your badge at your desk, visit the security office in the Metro lobby, 1st floor, to get a temporary one. Don't forget to return the temporary badge once you've retrieved your regular one. This process takes only a minute or two so there is no excuse for asking one of your co-workers to bend the rules for you.

Module 2, Screen 24:

Screen Title:

Alternative Workplaces

Screen Content:

Select the button that corresponds to your position to proceed

- FRs click here
- All others click here

Narration:

Working outside of a normal office environment presents a unique set of challenges for IT security and Data Stewardship. Field Representatives, click on the button marked "Field Representatives". Headquarters staff and all other personnel should click on the "All Others" button.

Module 2, Screen 25.1:

Screen Title:

Working in the Field

Screen Content:

- Don't allow others to see sensitive information on your device.
- Don't allow others to listen in as you ask respondents questions or review sensitive

paperwork, unless the respondent gives permission for others to remain in the room.

- Handle all PII with care
 - 11-39 forms
 - Performance Reviews
 - Doctor's Notes
 - Payroll Documentation
- Handle your device with care and protect against theft.
- Never allow anyone except a designated Census Bureau employee to repair your device.
- Make sure to keep the software and anti-virus programs up to date on all of your Census Bureau Devices.

Narration:

In the field, the burden of physically securing data falls on YOU. Whether in the field conducting interviews, making calls at your kitchen table, meeting with your supervisor in a public place, or handling the personal information of applicants or employees never allow people to see sensitive information on your device or allow others to listen in as you ask respondents' questions or review sensitive employee paperwork. If you are conducting an interview, the face-to-face contact you have with respondents means they are counting on YOU to keep their data safe. If someone else is in the room during an interview, make sure the respondent is comfortable doing the interview in their presence. Handle your own PII and PII of applicants and employees with the same care that you handle respondent PII. Lock up information such as job applications, 11-39 forms, performance reviews, doctor's notes, payroll documentation, or other employee paperwork. If you need to send PII to your supervisor by fax, make sure the intended recipient is there to receive it. If you email this information, make sure it is encrypted. Your device is a major target for theft, handle it with care. Never allow anyone except a designated Census Bureau Employee to repair your device. It is U.S. Government equipment. Make sure to keep the software and anti-virus programs up to date on all of your Census Bureau devices.

Module 2, Screen 25.2:

Screen Title:

All Other Alternative Workplaces

Screen Content:

- Keep your anti-virus software up-to-date
- Approved worksite only
- Access sensitive information ONLY through VDI or VPN, do not email it to yourself
- Handle all PII with care
- Do not take hard copies of Title 13 or Title 26 data home with you

Narration:

If you are authorized to work at an alternative work place, such as an approved telework location, please remember that you agreed to a special set of rules that specify what you may and may not do. Many of these rules are designed to protect sensitive data, and our IT systems. Always keep the anti-virus software up-to-date on the computer you use to make sure you don't inadvertently infect the Census Bureau network. You may not work at any location that is not approved such as a coffee shop, library, beach, or anywhere that you weren't specifically authorized to do so in your

telework or remote work agreement. NEVER email yourself files with sensitive information in them. You must only access sensitive information through the Virtual Desktop Infrastructure (also known as VDI) or the Census Virtual Private Network (also known as VPN). Also, never take hard copies of Title 13 or Title 26 out of Census Bureau buildings to work on them at home.

Module 2, Screen 26:

Screen Title:

Identifying and Reporting Information Security Incidents

Screen Content:

What is an Incident?

A security incident or data breach can include, but is not limited to:

- Sending or receiving an e-mail containing unencrypted sensitive PII/BII, Title 13, or Title 26 data.
- Letting an individual see sensitive information they're not allowed to see
- Discussing sensitive information with someone that isn't authorized to hear it
- Mishandled survey forms containing respondent information.
- Mishandled employee PII
- Removing Title 13 or Title 26 data from Census Bureau buildings or other approved work sites.
- Lost or stolen work laptop or other mobile device.
- Receiving a suspicious email asking for your personal information (Phishing).
- Receiving a phone call asking for your personal information.
- Suspicious behavior from computer or mobile device.

How do I handle an Incident?

Report both suspected and confirmed incidents to the BOC CIRT within one hour.

- **Headquarters:** 301-763-3333
- **RO Field Staff and After Hours Support for Headquarters and ROs:** 877-343-2010

- **Decennial Field Staff:** 855-236-2020 (24-hour support)
- Email BOC.CIRT@Census.gov (during business hours only)

Narration:

We have discussed the many policies and procedures the Census Bureau and YOU follow to ensure that data is safeguarded and an information security incident or breach is prevented. But what is considered an incident and how must you handle something you suspect to be an incident? Incidents and breaches can include, but are not limited to:

- Sending or receiving an e-mail containing unencrypted sensitive PII/BII, Title 13, or Title 26 data.
- Letting an individual see sensitive information they're not allowed to see
- Discussing sensitive information with someone that isn't authorized to hear it
- Mishandled survey forms containing respondent information.
- Mishandled employee PII
- Removing Title 13 or Title 26 data from Census Bureau buildings or other approved work sites.
- Lost or stolen work laptop or other mobile device
- Receiving an email asking for your personal information.
- Receiving a phone call asking for your personal information.
- Suspicious behavior from your computer or mobile device.

If you suspect something may be a security incident, even if you are unsure, contact the BOC CIRT and tell your supervisor within one hour of discovery.

Module 3

Module 3, Screen 27:

Screen Title:

IT Security Threats, Vulnerabilities and Countermeasures

Screen Content:

Learning Objectives

In this module you will learn about:

1. IT security threats
2. Vulnerabilities

Countermeasures including

- Following laws and policies designed to keep IT systems protected

- Hardware and software safeguards
- Requirements for creating secure passwords
- Procedures for using email safely
- Requirements for IT System Use

Narration:

You now understand your responsibilities when it comes to safeguarding data, but how can we do this when using IT systems comes with its own risks and challenges?

In this module you will learn about:

1. IT security threats
2. Vulnerabilities
3. And countermeasures including:
 - Following laws and policies designed to keep IT systems protected
 - Hardware and software safeguards
 - Requirements for creating secure passwords
 - Procedures for using email safely
 - Requirements for IT System Use

Module 3, Screen 28:

Screen Title:

Cyber Criminals Pose Threats...

Screen Content:

They try to:

- Take advantage of users and system vulnerabilities to gain unauthorized access
- Retrieve information for their own personal use
- Disrupt systems and alter data

Tools (that they use)

- Malware
- Social Engineering
- Phishing
- Spam

Narration:

Every day, there are around 16,000 attacks by cyber criminals on Census Bureau IT Systems. Cyber criminals are people who try to take advantage of users and system vulnerabilities to gain

unauthorized access to sensitive information, systems, and accounts. They may try to retrieve information for their own personal use or try to disrupt the system and alter the data. Some of the tools cyber criminals use to gain unauthorized access to computer systems are malware, social engineering, phishing, and SPAM. Let's learn more about each (of them).

Module 3, Screen 29:

Screen Title:

Malware

Screen Content:

Alias: Virus, Trojan Horse, Worm, Ransomware, Backdoor

Profile: Malicious Software designed to access sensitive information or damage our systems

Known for: Infecting your computer without your knowledge. There may be no sign that you downloaded or installed malware.

Caution: Installing unauthorized software on a Census Bureau System is not permitted. Also, do not click on links unless you are sure the site is safe

(Popup text) Viruses are self-replicating codes that operate and spread by modifying or damaging files and data. They are most frequently transmitted through e-mail attachments, but can also be transmitted by downloading malicious software from the Internet.

(Popup text) Worms are self-contained computer programs that are capable of spreading automatically. A worm uses network access to find a system with a vulnerability it can exploit and attacks the system with a virus or other malicious code. It then continues to look for more vulnerable systems to attack.

(Popup text) Trojan horses are programs containing malicious code that appear to be valid software applications. They are designed to trick users into copying and executing them.

(Popup text) Backdoors are tools cyber-criminals install to allow them to circumvent any security measures.

(Popup text) Ransomware is a software application that pretends to be something that it isn't. Most frequently seen in the form of fake anti-virus software.

Narration:

Malware, which is also called malicious code, is designed to allow unauthorized access to our information systems or cause intentional damage to our system or hardware. Malware can:

- Collect information from your computer without your informed consent
- Record your Internet surfing habits
- Interfere with your control of your computer (for example: Install additional software without your consent, redirect your web browser to other sites, change your computer settings)
- Impact your computer's performance (slow your connection speed, reduce or eliminate

internet or other computer functionality)

You can infect your computer with malware by installing a program that seems legitimate, such as a web accelerator or a helpful software agent, but actually has malicious code embedded within it. This is why installing unauthorized software on government equipment is not allowed.

You can also infect your computer if you click on a web page or link that connects you to a site that automatically downloads and activates malware on your computer. It is important to know that there may be no sign that you downloaded or installed malicious code. To be safe, avoid clicking on hyperlinks on web pages or emails unless you are sure the site the link directs you to is safe.

Module 3, Screen 30:

Screen Title:

Social Engineering

Screen Content:

Name: Social Engineering

Alias: Deceit, Impersonation, Trickery

Known for: Tricking people into giving out their personal or account information.

Caution: Never give out your username, password, or personal information unless you can verify the requester's identity and their need to know the information.

Narration:

Social engineering is a tool that cyber-criminals use to acquire sensitive information such as user names, passwords and credit card information from people.

Social engineering works through lies, deceit, impersonation and tricks. For example, a caller claims to be from the Help Desk and asks for your user name and password to install new software. If you give them this information, the cyber-criminal can now use your user name and password to act as you and gain access to sensitive information or perform other fraudulent activity.

This is why you should never give out your username, password, or personal information unless you can verify the requester's identity and their need to know the information

Module 3, Screen 31:

Screen Title:

Phishing

Screen Content:

Name: Phishing

Alias: Whaling, Spearphishing

Known For: Posing as a legitimate business, website, or organization.

- Caution: Messages may look like they come from the Census Bureau, your bank, your cable provider, or other legitimate businesses.
- Do not click on links or open attachments without carefully verifying they are from a reputable source.

(Popup Text) Spearphishing: Directed attack at a specific individual or company.

(Popup Text) Whaling: Directed attack at senior level officials or other high profile targets.

Narration:

Phishing is a form of social engineering that uses electronic means to get personal information. Two types of phishing are spearphishing and whaling.

Phishing scams rely on the victim trusting that an electronic communication or web site is legitimate. For example, a user clicks on a link in an email advertising a great vacation offer. The link takes the user to a fraudulent site that appears legitimate and asks them to enter personal information. If the user complies, the cyber-criminal can now steal the victim's identity or financial information for their own illegal use.

Scammers will try to make their messages look like they came from the Census Bureau, your bank or other legitimate businesses. Take great care and never click on links or open attachments without carefully verifying that they are from a legitimate source.

Module 3, Screen 32:

Screen Title:

Spam

Screen Content:

Name: Spam Alias: Junk Mail

Known for: Unsolicited email messages. Spam can serve as a vehicle for distributing malicious code or promoting phishing scams.

Caution: Do not download unsolicited programs or images or click on links in suspicious emails.

Narration:

Every email account, whether it be work or personal, receives a large number of unsolicited email messages. These unsolicited messages, known as junk emails or SPAM, can come in many forms. Most SPAM is filtered out before it even reaches your inbox, however, these filters cannot catch

everything. Be aware that SPAM can serve as a vehicle for distributing malicious code or promoting phishing scams. Be careful not to download unsolicited programs or images, or click on links in unsolicited or suspicious emails.

Module 3, Screen 33:

Screen Title:

Vulnerabilities

Screen Content:

(Images of tablet, smartphones, and laptop representing mobile devices)

- Computers
- Census Bureau Issued Devices
- Mobile Devices
- And Other Equipment

Narration:

All of the threats just discussed are tools criminals use to exploit vulnerabilities.

What are Census Bureau security vulnerabilities? Well, computers, Census Bureau issued devices, mobile devices, and other equipment are all vulnerable to unauthorized access or theft. To address this vulnerability, you are responsible for securing and limiting access to all government equipment.

Module 3, Screen 34:

Screen Title:

Laptops and Mobile Devices

Screen Content:

Laptops:

- Lock it up when not in use
- Follow acceptable use policies for what data may be stored on laptops
- Do not allow others to use your laptop
- Make sure no one can see your screen

Mobile Devices:

- Do not text sensitive data

- Do not use personal devices to take pictures, videos, or audio recordings where sensitive information is present
- Do not share your device

<link for the Policy for Audio, Video, and Photographs Captured Within Census Bureau Facilities Using a Personally Owned Device for internal users only)

Narration:

Laptop computers and mobile devices such as smartphones and tablets are tools that you may use to do your work regardless of where you are. However, these devices have some special rules about how they may be used. Some of these important rules are highlighted on this screen, but the Acceptable Use Policy that you will review at the end of this lesson contains all of the specific rules that govern your use of mobile devices you use as part of your job. In addition, you are not permitted to use personally-owned cell phones, cameras, or any recording devices to capture photographs, video, or audio in places where sensitive information is present or discussed. For example, do not record audio in the HRD call center or other telephone centers.

Do not take photos, audio, or video recordings of individuals inside Census Bureau facilities for work or personal purposes without their prior consent. For more information about the use of personally-owned devices, please see the Data Stewardship Policy for Audio, Video, and Photographs Captured within Census Bureau Facilities Using a Personally-Owned Device (internal use only policy).

Module 3, Screen 35:

Screen Title:

Social Media

Screen Content:

Social media includes:

- webinars
- blogs
- social communities
- wikis
- and video or photo sharing sites.

Social media use presents numerous IT vulnerabilities:

- Links on social media websites could take you to unintended locations
- Links could contain malware

- Code on the sites may prevent:
 - blocking ads
 - or other content that pose security risks.

Narration:

Social media is another vulnerability. Social media includes webinars, blogs, social communities, wikis, and video or photo sharing sites. All of these forms of social media can present a risk. Links on social media websites could take you to unintended locations or could contain malware. Also, the code on some social networking sites prevent the Census Bureau's firewall from blocking ads and other content that pose security risks.

Module 3, Screen 36:

Screen Title:

Peer-to-Peer Applications

Screen Content:

- Commercial peer-to-peer applications are not authorized for use at the Census Bureau unless approved by the Chief of the Office of Information Security.
- Only instant messaging through Census Skype for Business is allowed at the Census Bureau.

Narration:

Peer-to-peer applications are another vulnerability. They include instant messaging like Google Hangouts and Facebook chat, and file sharing programs like OneDrive, Dropbox, and BitTorrent. Applications like these are a risk for computer systems because they allow internet users to share files that are housed on their computers. Shared files often come with malware, backdoors, viruses, or other malicious content attached to them.

Commercial peer-to-peer applications are not authorized for use at the Census Bureau unless approved by the Chief of the Office of Information Security. ONLY instant messaging through Census Skype for Business is allowed at the Census Bureau.

Module 3, Screen 37:

Screen Title:

Laws Designed to Protect IT Systems

Screen Content:

E-Government Act Requirements

- Privacy policy posted on public website
- Conduct Privacy Threshold Analysis (PTA)/Privacy Impact Assessments (PIAs) before developing, obtaining, or revising IT systems that contain PII/BII.

Federal Information Security Management Act (FISMA)

- Part of the E-Government Act
- Requires federal agencies to develop, document and implement an agency-wide information security program to protect their information systems and the data they contain

For more information about privacy requirements of the E-government Act, contact the Census Bureau Privacy Compliance Branch at 301-763-6440. For more information about FISMA requirements, contact the Office of Information Security at 301-763- 2862.

Narration:

Now that we talked about the threats, let's talk about laws and countermeasures that protect our IT Systems. Countermeasures begin by following IT security laws.

The E-Government Act requires every agency to create a privacy policy and post it to their public website.

It also requires agencies to conduct Privacy Impact Assessments (or PIAs) before developing, obtaining, or revising any IT systems that contain PII/BII. PIAs ensure the IT system has sufficient privacy protections for the personal information contained in it. The E-Government Act also requires that the Census Bureau make PIAs publicly available. A Privacy Threshold Analysis (PTA) should be completed to determine whether a PIA is required.

As part of the E-Government Act, the **Federal Information Security Management Act, (or FISMA)** requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information systems and the data they contain. If you are responsible for developing, acquiring, or revising IT systems, or for more information about privacy requirements of the E-government Act, contact the Census Bureau Privacy Compliance Branch at 301-763-6440.

For more information about FISMA requirements, contact the Office of Information Security.

Module 3, Screen 38:

Screen Title:

Hardware and Software Safeguards

Screen Content:

All requests must be reviewed and processed by the Standards Working Group. They ensure software:

- Meets Census Bureau standards
- Is the most efficient use of funds
- Is the most effective use of IT resources
- Meets security requirements

Never install unauthorized software.

Narration:

Hardware and software safeguards protect our computers, devices, and IT systems.

The Standards Working Group or SWG is a chartered body that reviews IT product requests for hardware and software. All requests for software must be processed through the SWG. This procedure ensures the software meets Census Bureau standards, is the most efficient use of funds for software purchases, and is the most effective use of IT resources. More importantly, this process ensures that any software we use meets security requirements under the US Government Configuration Baseline.

As a reminder, you should **NEVER** install unauthorized software to any Census Bureau computer or device.

Module 3, Screen 39:

Screen Title:

Passwords

Screen Content:

- Do NOT create weak passwords that are easily guessed.
- Do NOT use your name or other PII such as your birth date to design a password.
- Do NOT write passwords down, store them, or set applications to remember your password.

- Do NOT share your passwords with anyone except authorized Census Bureau personnel such as IT staff. After the need is over, you must change your password immediately.
- DO create passwords that meet Department of Commerce and Census Bureau requirements.
- DO change your passwords regularly.
- DO report compromised passwords to the Bureau of Census Computer Incident Response Teams or BOC CIRT. They will suspend your account until the issue is resolved, then you may call to have it re-enabled.
- DO avoid emailing passwords. If you absolutely must email a password, use secure encryption with Secret Agent or Kiteworks and do not include the user ID in the same message.
- DO use different passwords for different applications. By having different passwords, if one password is compromised, they're not all compromised.

Review the Department of Commerce policy on Password Management <Link to the Password Management Policy. This is Appendix D.>

Narration:

It is up to you to create strong passwords and protect them from disclosure and unauthorized use. To protect your passwords:

- Do NOT create weak passwords that are easily guessed.
- Do NOT use your name or other PII such as your birth date to design a password.
- Do NOT write passwords down, store them, or set applications to remember your password.
- Do NOT share your passwords with anyone except authorized Census Bureau personnel such as IT staff. After the need is over, you must change your password immediately.
- DO create passwords that meet Department of Commerce and Census Bureau requirements.
- DO change your passwords regularly.
- DO report compromised passwords to the BOC CIRT. They will suspend your account until the issue is resolved, then you may call to have it re-enabled.
- DO avoid emailing passwords. If you absolutely must email a password, use secure encryption programs such as Secret Agent or Kiteworks, and do not include the user ID in the same message.
- DO use different passwords for different applications. By having different passwords, if one password is compromised, they're not all compromised.

For more information, please review the Department of Commerce policy on password management (this is Appendix D).

Module 3. Screen 40:

Screen Title:

Email Use

Screen Content:

- Header
- Body
- Attachments

Narration:

Email is one of the most common ways for cyber-criminals to stage their attacks. Click each section of the email to learn how to use email appropriately.

Click the link to learn more about the procedures for reporting unsolicited emails.

Module 3. Screen 40.1:

Screen Title:

Header

Screen Content:

When receiving an email, make sure you trust the sender and that the subject line of the email seems legitimate.

You should ask yourself questions like:

- Do I know the person sending me this email?
- Does this email address seem legitimate?
- Is the subject of this message something this person would be contacting me about?
- Did I sign up for the service that is sending me this email?
- Is this email referencing an account that I don't have?
- Should I be receiving emails about this on my work email account?

If these things don't check out, don't open the email but also don't delete it. The email could be spam, a phishing scam, or may contain malicious code and should be reported to the BOC CIRT. Appendix G contains instructions on what you should do if you receive unsolicited emails

Module 3. Screen 40.2:

Screen Title:

Attachments

Screen Content:

Email attachments are one of the easiest ways for cyber criminals to infect your computer with malicious code. Before opening an attachment, ask yourself the following questions:

- Does the file name of this attachment make any sense?
- Does this attachment make sense in the context of this email?
- Does the file extension correspond with what the attachment is supposed to be?
 - For example, if the attachment is supposed to be a PowerPoint presentation, it should end in .pptx, not .exe

Don't open email attachments that you don't trust. Report this email to the BOC CIRT. See Appendix G for instructions on reporting suspicious email.

Module 3. Screen 40.3:

Screen Title:

Body

Screen Content:

If the email header checks out ok and you've opened the message, you should always check the body of the email to make sure it's legitimate. Even if you trust the sender, there is a chance that their email account may have been compromised. Cyber criminals will use the address book of a compromised email account to spam other email accounts with malicious code or phishing scams since users are more likely to fall victim to these attacks if they trust the sender.

When you open an email you should ask yourself the following questions:

- Is this something I would expect this person to contact me about?
- Is the sender asking me for sensitive information?
- Does this email "sound" like the sender?
- Are there any suspicious links that the email asks me to click on?
- Is the email blank, but there is an attachment at the end?

If any of these areas don't check out, don't delete the email. You should report this email to the BOC CIRT. See Appendix G for instructions on reporting suspicious email.

Module 3, Screen 41:

Screen Title:

Email Use

Screen Content:

Sensitive information in Email

- If the sender included any sensitive information in an email, report it to BOC CIRT.
- Never include any sensitive information (including your own PII) in the body of a message.
- Emails that might contain sensitive PII will be reviewed and quarantined.
- Avoid emailing usernames and passwords.

Sensitive Information in Attachments

- Send sensitive information as an encrypted attachment using Census approved encryption tool such as Secret Agent or Kiteworks.
- If an attachment is legitimate, but it contains unencrypted sensitive information related to your Census Bureau work, report it to BOC CIRT.

Narration:

Even if the email is legitimate, if the sender included any sensitive information, even their own sensitive PII, report the email to the BOC CIRT. Also, never send YOUR OWN PII in the body of an email. When sending an email never include any sensitive information such as respondent names or addresses in the body of the message. Avoid emailing sensitive information whenever possible, but, if you must, send it as an encrypted attachment. Census Bureau scans all messages sent from census.gov email addresses to make sure they don't contain any sensitive PII. Emails that might contain sensitive PII will be reviewed and those that have it will be quarantined. If one of your emails is quarantined, you will be notified. Avoid emailing usernames and passwords. If you must, send the username and password in separate emails.

When emailing sensitive information from your Census Bureau email address, send it as an encrypted attachment using Census approved encryption tools such as Secret Agent or Kiteworks.

If you receive an attachment that contains unencrypted sensitive information report the email to the BOC CIRT.

Module 3, Screen 42:

Screen Title:

Email Use

Screen Content:

If you have a Census.gov email address:

- Use for official business only
- Never use to sign up for social media, commercial, or any other personal accounts
- Never use your personal email for official business
- Do not auto-forward to a non-Census Bureau account

Narration:

If you have a census.gov email address, make sure you use for official business only. All email sent or received through your census.gov email account may be considered property of the Census Bureau, may be considered an official record, and could be requested under the Freedom of Information Act.

Also, make sure that you never use your personal email account for official business. Always use your census.gov email address for work-related communications.

Auto-forwarding emails you receive to an account outside the Census Bureau network is prohibited. However, setting up an Auto-reply message when you are out of the office or on vacation is permitted.

Module 3, Screen 43:

Screen Title:

Reporting Security Incidents

Screen Content:

Report incidents to the BOC CIRT within 1 hour.

- Headquarters: 301-763-3333
- RO Field Staff and After Hours Support for Headquarters and ROs: 877-343-2010
- Decennial Field Staff: 855-236-2020 (24-hour support)
- Email BOC.CIRT@Census.gov (during business hours only)

When reporting an incident, include:

- Name of individual involved in incident

- Location of incident
- Time of incident
- Summary of incident
- Identify lost or disclosed PII
- A Police Report (If there is one)
- Scope or extent of the loss or disclosure

Report suspicious emails BEFORE you open them.

Report any suspicious behavior from your computer or device.

Do not send a report via email from a computer that may be compromised.

Narration:

The BOC CIRT is dedicated to preventing incidents and limiting the damage should they occur. They are here to help you.

Contact them within one hour if you suspect a cyber-attack or information security incident. You should also inform your supervisor.

When reporting the incident, include the following details.

- Name of individual involved in incident
- Location of incident
- Time of incident
- Summary of incident
- Identify lost or disclosed PII
- A Police Report (If there is one)
- Scope or extent of the loss or disclosure

Report suspicious emails BEFORE you open them.

Report any suspicious behavior from your computer or device.

Do not send a report via email from a computer that may contain a virus or malicious code.

Module 3, Screen 44:

Screen Title:

IT Systems Acceptable Use

Screen Content:

Personal use must not:

- Interfere with official duties
- Create the impression that the individual's personal views or activities represent the Census Bureau

- Pose a security risk
- Consume excessive resources
 - Using work Email for Personal Use
 - Video Streaming
 - Music Streaming
 - Personal Printing

There is no right to privacy in Census Bureau It Systems. Your use may be monitored at any time. (Click here to) Read the IT Acceptable Use Policy.

Narration:

Using Census Bureau Internet access and related computer resources for purposes other than official business is only permitted if you are on non-duty time during business hours or have approval from your supervisor. This limited personal use of e-mail, Internet access, computer resources, networks, and printers must not:

- Interfere with your official duties
- Create the impression that your personal views or activities represent the Census Bureau
- Pose a security risk or
- Consume excessive resources

Excessive resource use includes such activities as: filling an e-mail box with personal messages, creating or transmitting personal mass mailings or chain letters, downloading or sending large personal files via e-mail, or downloading large non-work-related audio or video streams.

There is no right to privacy in Census Bureau IT systems and that your use of IT resources may be monitored for compliance with IT security policies at any time.

To continue this course, please read the IT Acceptable Use Policy. After reading it, you must click to acknowledge that you have read and accept the terms of the IT Acceptable Use Policy.

[For the text-based version of the training, by signing your Data Stewardship Training certificate, you agree that you have read and accept the terms of the IT Acceptable Use Policy.]

Module 3, Screen 45:

Screen Title:

Conclusion

Screen Content:

You learned about:

- Privacy and data stewardship
- Data protection and the law

- Safeguarding data.
- IT security threats, vulnerabilities, and countermeasures.

< Link to Glossary. This is Appendix G >

Narration:

You've reached the end of this training. You now have a solid understanding of privacy and data stewardship; data protection and the law; IT security threats and vulnerabilities and countermeasures; and safeguarding data. For future reference, click the link for a glossary of terms used in this training. [The Glossary can be found in Appendix G of this document.] Click Next to begin the Knowledge Check for this course.

Final Assessment, Introduction Screen:

Screen Title:

Pulling It All Together: Final Assessment

Narration:

It's time to assess your understanding of the material presented. Please read the directions and select the correct answer(s). Please make sure you read the directions for each question as some questions have more than one correct answer.

To receive credit for completing this module, you must receive a score of 70% or higher.

Knowledge Check, Question 1:

Instructions:

Choose the correct answer.

Question:

Who is ultimately responsible for following all regulatory requirements and internal policies and standards for how data are handled?

- A. The Census Bureau
- B. The Department of Commerce
- C. You
- D. System Owners

Knowledge Check, Question 2:

Instructions:

Choose the correct answer.

Question:

Why do we practice good data stewardship?

- A. To keep the public's trust
- B. The law requires it
- C. To protect individuals from identity theft
- D. All of the above

Knowledge Check, Question 3:

Instructions:

Choose the correct answer.

Question:

Title 13 is the law that authorizes and directs the Census Bureau to conduct censuses and surveys and sets forth the standards of confidentiality for our data. What are the penalties for unauthorized disclosure under Title 13?

- A. Up to 5 years in prison and up to \$250,000 in fines
- B. Up to 22 years in prison and fines in excess of \$600,000
- C. Administrative reprimand and civil liabilities.

Knowledge Check, Question 4:

Instructions:

Choose the correct answer.

Question:

Which law protects the personal information YOU provide the Census Bureau as part of your employment?

- A. CIPSEA
- B. Title 13
- C. FISMA

D. Title 5

Final Assessment, Question 5:

Instructions:

Choose all of the correct answers to the following question. One or more answers may be correct.

Question:

When you began working for the Census Bureau, you took an oath of non-disclosure. When does your obligation to protect sensitive information you encounter as part of your job end?

- A. Immediately after my work with the Census Bureau ends
- B. When I log out at the end of the day
- C. When I retire
- D. Never

Final Assessment, Question 6:

Instructions

Choose the correct answer to the following question.

Question

If you are unsure whether the information you're working with is sensitive or not, you should...

- A. Assume it's public information
- B. Ask your supervisor
- C. Show it to and ask your peers
- D. Guard it with your life

Final Assessment, Question 7:

Instructions

Choose the correct answer to the following question.

Question

Cyber criminals use many different methods to gain access to information systems and the sensitive information on those systems. Malware, or malicious code, is one form used by criminals. Which of the following are ways you might accidentally infect your computer with malware?

- A. By clicking on a link that appears legitimate, but downloads and activates malware on your computer
- B. By installing unauthorized software on your Census Bureau computer
- C. By installing what appears to be a legitimate program such as a web accelerator, but has malicious code embedded
- D. By opening email attachments that contain malicious code

Final Assessment, Question 8:

Instructions

Choose the correct answer to the following question.

Question

Which of the following are true about Phishing scams?

- A. The sender of the message may be, or appear to be, someone you know.
- B. There may be a link to a website that appears legitimate.
- C. The email may ask you for your account information.
- D. All of the Above

Final Assessment, Question 9:

Instructions

Choose the correct answer to the following question.

Question

What type of cyber-crime works through lies, deceit, impersonation and tricks to obtain access to user names, passwords, and credit card information?

- A. Social Engineering
- B. Malware
- C. Spam
- D. Trojan Horses

Final Assessment, Question 10:

Instructions:

Choose all of the correct answers to the following question. One or more answers may be correct.

Question:

Which of the following should be locked when not in use?

- A. Your workstation
- B. Your pod or office
- C. Your device
- D. All of the above

Final Assessment, Question 11:

Instructions:

Choose all of the correct answers to the following question. One or more answers may be correct.

Question:

If you have access to sensitive information, you may... (Choose all that apply)

- A. Browse it freely.
- B. Access it only if you have a work-related need to know that information.
- C. Share it with a coworker because it is interesting.
- D. Share it with a coworker who has a work-related need to know the information.

Final Assessment, Question 12:

Instructions:

Choose whether the following statement is true or false.

Question:

True or False: You DO NOT have a right of privacy in Census Bureau IT systems.

- A. True
- B. False

Final Assessment, Question 13:

Instructions:

Choose the correct answer to the following question.

Question:

There are limitations to how you may use social media while working for the Census Bureau. Unless authorized, which of the following are NOT PERMITTED?

- A. Contacting respondents on social media
- B. Signing up for social media accounts on behalf of the Census Bureau
- C. Signing up for social media accounts using @census.gov email address
- D. All of the above

Final Assessment, Question 14:

Instructions:

Choose whether the following statement is true or false.

Question:

Sometimes passwords can be long, complicated, and difficult to remember. To make sure you do not forget your passwords you should...

- A. Write them down
- B. Set applications to remember them
- C. Use the same password for every application
- D. None of the above

Final Assessment, Question 15:

Instructions:

Choose the correct answer to the following question.

Question:

What is the time requirement for reporting a suspected or confirmed data breach, or a lost or stolen Census Bureau-issued device?

- A. As soon as you have time
- B. No later than the next business day
- C. Within an hour after you identify or discover the loss of a device or data

Final Assessment, Question 16:

Instructions:

Choose all of the correct answers to the following question. One or more answers may be correct.

Question:

Any time you ship hard copies of sensitive information, you should...

- A. Double-wrap the package.
- B. Send it using an approved carrier.
- C. Insure the shipment for \$1,000.

Final Assessment, Question 17:

Instructions:

Choose the correct answer to the following question.

Question:

You lost a printout containing Title 13 information. Your boss is out on vacation until tomorrow. You should...

- A. Wait until tomorrow to call the BOC CIRT so you can let your boss know first.
- B. Call BOC CIRT within one hour of discovering the lost printout.
- C. Keep looking for a few more hours, maybe you'll find the printout and won't have to report it.

Final Assessment, Question 18:

Instructions:

Choose the correct answer to the following question.

Question:

While walking into an empty bathroom in a Census Bureau office building, you see a stack of employment applications with names, addresses and other information on them. What do you do?

- A. Leave it for the person to come back and find it.
- B. Take it to Lost and Found.
- C. Wait to talk to your boss about it when she comes back from an off-site.
- D. Take the applications back to your desk and call BOC-CIRT within 1 hour.

Final Assessment, Question 19:

Instructions:

Choose the correct answer to the following question.

Question:

You were issued a Census Bureau device and you've lost it. You tried calling your supervisor but she hasn't called you back yet. You should

- A. Wait to call the BOC CIRT until you hear from your Census supervisor
- B. Call the BOC CIRT within one hour of the loss of your device
- C. Keep looking for the device for a few more hours. Maybe you will find it and you won't have to report it.

Final Assessment, Question 20:

Instructions:

Choose all of the correct answers to the following question.

Question:

True or False: You should only report confirmed data security incident to the BOC CIRT. If you don't know for sure that sensitive data was lost you, you should investigate the issue first.

- A. True
- B. False

Final Assessment, Question 21:

Instructions:

Choose all of the correct answers to the following question.

Question:

You receive a call to your work telephone number from someone saying they are from IT and your computer has been infected with a virus. The person asks you for your password or Social Security Number. What should you do?

- A. Hang up immediately.
- B. Provide the requested information, then report it to BOC CIRT.
- C. Do not provide the information- gather and write down as much information about the call as you can and report it to the BOC CIRT.

Final Assessment, Question 22:

Instructions:

Choose the correct answer to the following question.

Question

You receive a suspicious email or message on your Census Bureau computer or device, asking you to confirm the contact information for a bank account. What should you do?

- A. Delete the email.
- B. Provide the requested information.
- C. Call the BOC CIRT

Final Assessment, Question 23:

Instructions:

Choose the correct answer to the following question.

Question

You log back into your computer or device after a meeting and find a popup up window. It keeps coming back even after you hit the close button. This could be a sign of Malware. What do you do?

- A. Hit Ctrl-Alt-Del and shut down your computer or device.
- B. Call BOC-CIRT.
- C. Talk to your colleague who is savvy about computers or devices freezing up.
- D. Wait to talk to your boss about it when she comes back from an off-site.

Final Assessment, Question 24:

Instructions:

Choose all of the correct answers to the following question. One or more answers may be correct.

Question:

It's a pretty Saturday morning and you're out in the field conducting interviews. As you approach a respondents' front door, somebody runs by and snatches your laptop. What should you do?

- A. Run after them!
- B. Call the police.
- C. Call your supervisor.
- D. Call BOC CIRT within one hour.

Final Assessment, Question 25:

Instructions:

Read this transcript of an email message and then answer the following question.

Email Message:

Subject: IT Maintenance Schedule From: CensusHelpDesk@hotmail.com

To: steward.data@census.gov

This week we are performing routine maintenance on all user accounts. To minimize disruption and make it easier for you, please click on the link below and provide the information requested to confirm that your account is still active.

<http://www.censushelpcenter.uk>

Census Bureau Help Desk Staff

Question:

What if anything looks suspicious about this email that would cause you to report it to BOC CIRT? Choose all that apply.

- A. Sender's Email Address
- B. Poor grammar in the body of the email
- C. The email attachment
- D. The link in the email message
- E. There is no reason to report this email.

Final Assessment, Question 26:

Instructions:

Read this transcript of an email message and then answer the following question.

Email Message:

Subject: Urgent: Payroll Verification From: steward.data@census.gov

To: HRD Call Center/BOC

To HR Help Desk,

The direct deposit for my paycheck wasn't processed this pay period. Please look into it. Here is my Social Security Number if you need it: ###-##-####

And here's my bank account and routing numbers: ##### - #####

Thanks,

Steward

Question

What if anything about this email would cause you to report it to BOC CIRT? Choose all that apply.

- A. Sender's Email Address
- B. PII was sent in the body of the email message
- C. The email attachment
- D. The subject line
- E. There is no reason to report this email

Final Assessment, Question 27:

Instructions:

Read this transcript of an email message and then answer the following question.

Email Message:

Subject: Thursday Meeting From: joe.coworker@census.gov To: steward.data@census.gov Hey, Hey Stewie,
Did you get everything ready for the meeting with Bill on Thursday?
BTW, you gotta try this program I found. It really increased the speed of my computer.
Attachment: WebAccelerator.exe

Question

What if anything about this email would cause you to report it to BOC CIRT?

- A. Sender's Email address
- B. PII was sent in the body of the email message
- C. The email attachment
- D. The subject line
- E. There is no reason to report this email

Final Assessment, Question 28:

Instructions:

Choose the correct answer to the following question

Question:

Does the following require secure disposal?
An employment application with name, address, and date of birth

- A. Yes
- B. No

Final Assessment, Question 20:

Instructions:

Choose all of the correct answers to the following question. One or more answers may be correct.

Question:

Does the following require secure disposal?

A printout containing Tile 13 data

- A. Yes
- B. No

Module 3, Screen 46:

Screen Title:

Congratulations and Title 26 full training reminder

Screen Content:

Please note you must complete additional Title 26 Training if you work at:

- Census Bureau Headquarters
- National Processing Center (NPC)
- Bowie Computer Center
- Federal Statistical Research Data Centers
- And anywhere else that Federal Tax Information is accessed.

Contact your Supervisor, Sponsor, or Contracting Officer's Representative (COR) COR for instructions. Field Representatives (FRs), Enumerators, and Regional Staff (RO) staff generally do NOT need additional Title 26 training.

Module 3, Screen 47:

Screen Title:

Section 508 Compliance

Screen Content:

Section 508 of the Rehabilitation Act of 1973 requires Federal agencies to ensure their Information and Communication technology (ICT) are accessible to persons with disabilities, while providing access to and use of information and data that is comparable to that provided to persons without disabilities. ***ICT access for all users is a statutory requirement.***

Section 508 affects many different people, in many roles, and in many different parts of the organization. All Federal employees and contractors are responsible for Section 508 compliance that aligns with their role in the organization.

Learn to do your part. Sign up for one or more Section 508 training courses on the Commerce Learning Center:

- Section 508 – An Overview (no prerequisite course required)
- Section 508 Coding Fundamentals for Developers (no prerequisite course required)

Contact the Section 508 Program Office: (301) 763-1508

census.508.accessibility@census.gov

Final Assessment, Answer Key:

Answers:

1. C
2. D
3. A
4. D
5. D
6. B
7. A, B, C, D
8. D
9. A
10. D
11. B, D
12. A
13. D
14. D
15. C
16. A, B
17. B
18. D
19. B
20. B
21. C
22. C
23. B
24. B, C, D
25. A, D
26. B
27. C
28. A
29. A

Appendix A Updated September 2019

Data/Information Handling Guidelines

This attachment provides specific guidelines for handling each type of sensitive information in use at the Census Bureau. For each information type, this section discusses Creation, Storage, Printing, and Disposal.¹

Data/Information Type	Electronic Transmission	Printing and managing paper copies	Disposal
<p>Title 13</p> <p>Electronic or paper documents must be labeled "Disclosure Prohibited – Title 13 U.S.C." or similar.</p>	<p>Encrypt before transmission using an approved encryption method, such as WinZip encryption. Send as attachment, not in the body of an email.</p> <p>Department of Commerce Kiteworks software https://sfc.doc.gov/ is also authorized for encryption and transmission.</p> <p>If teleworking or working remotely, only access Title 13 information in VDI or through your VPN connection if using a Census-issued laptop —do not email Title 13 information to yourself for use at home.</p> <p>Only Skype for Business is authorized for teleconferencing with Title 13 Information. See the Skype for Business with Title 13 Data and Sensitive PII guidance for more instructions. (https://collab.ecm.census.gov/teamsites/O365P/planning/SfBTrain/Pages/Title-13-and-Sensitive-PII.aspx)</p> <p>If faxing, ensure someone is at the machine to receive it and confirm receipt after sending.</p>	<p>Print with a cover page or with private printing.</p> <p>Immediately remove printouts from printer.</p> <p>Keep locked in desk or file cabinet when not in use.</p> <p>Restrict access to only those Census Bureau staff and contractors or other individuals with Special Sworn Status and with a business need to know.</p> <p>Do not remove hard copies from secure Census Bureau facilities, even for telework.</p>	<p>Dispose of hard copies in a locked blue bin designated for sensitive materials.</p> <p>Field staff should follow guidance on shipping materials to the Regional Office for destruction.</p> <p>Dispose of electronic copies (tapes, cds, disks, etc.) in locked blue bin or by contacting the Records Office at 3-2282.</p>

¹ Note: as the Census Bureau moves in phases to implement Controlled Unclassified Information (CUI) standards and markings this document will be updated.

Appendix A

Data/Information Type	Electronic Transmission	Printing and managing paper copies	Disposal
<p>Title 26</p> <p>Electronic or paper documents <u>must be labeled</u> "Disclosure Prohibited – Federal Tax Data Protected by Title 26 U.S.C."</p>	<p>Encrypt before transmission using an approved encryption method, such as WinZip encryption. Send as attachment, not in the body of an email.</p> <p>Department of Commerce <u>Kiteworks</u> software (https://sfc.doc.gov/) is also <u>authorized</u> for encryption and transmission.</p> <p>If teleworking or working remotely, only access Title 26 information in VDI or through your VPN connection if using a Census-issued laptop —do not email Title 26 information to yourself for use at home.</p> <p>Contractors and SSS are <u>NOT</u> <u>authorized</u> to work remotely with Title 26 information.</p> <p>Title 26 information is <u>NOT</u> <u>authorized</u> for use in any videoconferencing applications, even Skype for Business.</p> <p>If faxing, ensure someone is at the machine to receive it and confirm receipt after sending.</p>	<p>Print with a cover page or with private printing.</p> <p>Immediately remove printouts from printer.</p> <p>Log printing in print logs near the printers to ensure tracking of hard copies.</p> <p>Keep locked in desk or file cabinet when not in use. File cabinet <u>must be labeled</u> as containing Title 26 information.</p> <p>Restrict access to only those Census Bureau staff and contractors or other individuals with Special Sworn Status with a business need to know who are on an approved Title 26 project.</p> <p>Do not remove hard copies from secure Census Bureau facilities, even for telework.</p>	<p>Dispose of hard copies in a locked blue bin designated for sensitive materials.</p> <p>Log disposal and destruction of all hard copies using disposal logs located in printing rooms.</p> <p>Dispose of electronic copies (tapes, <u>cds</u>, disks, etc.) in locked blue bin or by contacting the Records Office at 3-2282.</p>

Appendix A

Data/Information Type	Electronic Transmission	Printing and managing paper copies	Disposal
Title 5 / Sensitive PII	<p>Encrypt before transmission using an approved encryption method, such as WinZip encryption. Send as attachment, not in the body of an email.</p> <p>Department of Commerce <u>Kiteworks</u> software (https://sfc.doc.gov/) is also authorized for encryption and transmission.</p> <p>If teleworking or working remotely, only access Title 5 information in VDI or through your VPN connection if using a Census-issued laptop —do not email Title 5 information to yourself for use at home.</p> <p>Only Skype for Business is authorized for teleconferencing with Title 5 data. See the <u>Skype for Business with Title 13 Data and Sensitive PII</u> guidance for more instructions (https://collab.ecm.census.gov/teamsites/O365P/planning/SfBTrain/Pages/Title-13-and-Sensitive-PII.aspx). If faxing, ensure someone is at the machine to receive it and confirm receipt after sending.</p>	<p>Print with a cover page or with private printing.</p> <p>Immediately remove printouts from printer.</p> <p>Keep locked in desk or file cabinet when not in use.</p> <p>Restrict access to only those Census Bureau staff, contractors, or other individuals with a business need to know.</p>	<p>Dispose of in locked blue bin or shred with an approved <u>cross-cut shredder</u>.</p> <p>Field staff should follow guidance on shipping materials to the Regional Office for destruction.</p> <p>Dispose of electronic copies (tapes, <u>cds</u>, disks, etc.) in locked blue bin or by contacting the Records Office at 3-2282.</p>

Appendix A

Data/Information Type	Electronic Transmission	Printing and managing paper copies	Disposal
<p>Administratively Restricted</p> <p>Electronic or paper documents may be labeled “For Official Use Only”, “For Internal Use Only” or similar.</p>	<p>Encrypt if the sensitivity level is high; check with your supervisor.</p> <p>Transmit with care if not encrypting – ensure that the individual receiving the email is aware of the sensitive nature of the document.</p> <p>If faxing, ensure someone is at the machine to receive it.</p>	<p>Can print without restrictions.</p> <p>Keep hidden from view when members of the public are present.</p> <p>Keep locked when not in use if warranted; check with your supervisor if unsure of the sensitivity of a particular item.</p> <p>Label ‘for internal use only’ or something similar to designate it as a non-public document.</p>	<p>Dispose of in locked blue bin, not regular recycling.</p> <p>Dispose of electronic copies (tapes, cds, disks, etc.) in locked blue bin or by contacting the Records Office at 3-2282.</p>
Public Use	No handling restrictions – Do not send to the public without permission from your supervisor.	No handling restrictions – Do not release to the public without permission from your supervisor.	Dispose in locked blue bins.

Appendix A

Mailing and Shipping Instructions

Data/Information Type	Mailing and Shipping
Title 13	<p>When mailing or shipping Title 13 Controlled information, the media (paper documents, hard drives, DVDs, etc.) must be double wrapped and shipped using an approved traceable carrier.</p> <p>The outer wrapping must specify that the package or envelope is for delivery only to a specific recipient, preferably an individual where possible. The outer wrapping should be opaque and NOT indicate that the package or envelope indicating it contains Title 13 information.</p> <p>The inner wrapping must be opaque, tamper-evident, and be labeled "This package contains information legally protected by Title 13 U.S.C. To be opened by addressee only."</p>
Title 26	<p>When mailing or shipping Title 26 information, the media (paper documents, hard drives, DVDs, etc.) must be double wrapped and shipped using an approved traceable carrier.</p> <p>The outer wrapping must specify that the package or envelope is for delivery only to a specific recipient, preferably an individual where possible. The outer wrapping should be opaque and NOT indicate that the package or envelope indicating it contains Title 26 information.</p> <p>The inner wrapping must be opaque, tamper-evident, and be labeled "This package contains information legally protected Title 26 U.S.C.) To be opened by addressee only."</p>

U.S. Department of Commerce
Office of Digital Engagement
Policy on the Approval and Use of
Social Media and Web 2.0 (SM/W2.0)

TABLE OF CONTENTS

Why This Policy Is Necessary71

 SM/W2.0 Technologies:.....72

 Purpose and Goals:.....72

General Guidelines for the Use of SM/W2.0 Technologies in an Official Capacity:73

 (1) Department Employees:73

 (2) Guidelines for Use of SM for Operating Units:75

 (3) Hatch Act in the Workplace:77

Applying for Official SM/W2.0 Accounts77

General Guidelines for the Use of SM/W2.0 Technologies in an Unofficial Capacity:77

 (1) Personal and Professional Communication:77

 (2) Employee Title Use:78

 (3) Hatch Act on Personal Accounts:79

Other Applicable Commerce Policies80

Responsibilities of Chief Information Officers80

 Risk Assessment and Authorization for Use:.....80

 Terms of Service and Privacy:81

Specific IT Security Guidelines for Using SM/W2.0 Technologies81

Resources for Additional Information82

Why This Policy Is Necessary

The Department of Commerce is committed to operating all its communications and transactions with individuals and organizations in an open and transparent way. Social media and Web 2.0

(SM/W2.0) services are an increasingly important avenue for stakeholders and members of the public to interact with the Department in an efficient, effective, and transparent manner.

SM/W2.0 Technologies:

SM/W2.0 services encompass many technologies, including XML feeds, wikis, blogs, social networking sites, discussion forums, collaborative research Web sites, comment features on news and video Web sites, and other mechanisms. Social media services allow the user to interact directly with the Web site or other users. The result is that Web users are able to communicate simultaneously, directly, and instantaneously with all other users on the Web site. Commonly used social media services include YouTube®, Flickr®, Facebook®, Twitter®, and Instagram®.

SM/W2.0 technologies also present new and unprecedented challenges to the security of the information technology (IT) networks and systems that Commerce and its operating units use, as well as complicate the protection of personally identifiable information (PII). Commerce's and other Federal agencies' information systems are targeted by persistent, pervasive, and aggressive threats. These threats may be directed against the network infrastructure or IT systems, as well as records or information in the systems, especially PII or other sensitive information. The rapid development of Web 2.0 technologies and their emerging capabilities and uses present new and ever increasing risks that require continuing vigilance by IT security personnel and employees who use SM/W2.0 services.

Purpose and Goals:

The purpose of this policy is to provide guidance for operating units and Commerce employees to take full advantage of SM/W2.0 technologies while, at the same time, protecting Commerce and its employees by mitigating risks inherent in using these services.

This policy conforms to and implements the following:

- [Guidelines for Secure Use of Social Media by Federal Departments and Agencies](#) that were adopted by the Chief Information Officers (CIO) Council and issued in September 2009.
- [President's Memorandum on Transparency and Open Government](#), calling for openness in Government and the establishment of a system of transparency, public participation, and collaboration, January 21, 2009.
- Office of Management and Budget (OMB) [Memorandum M-10-23](#), Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010.
- National Archives and Records Administration (NARA) [Bulletin 2011-02](#), Guidance on Managing Records in Web 2.0/Social Media Platforms, October 20, 2010.
- [OMB's Digital Government Strategy](#), May 2013

- United States Office of Government Ethics' [LA-15-03: The Standards of Conduct as Applied to Personal Social Media Use](#), April 2015

General Guidelines for the Use of SM/W2.0 Technologies in an Official Capacity:

While the following section discusses specific requirements for Department employees and operating units, each requirement is applicable to all Department operations.

(1) Department Employees:

The following are general guidelines for Department employees assigned official responsibility for operating an official account or contributing to a SM/W2.0 Web site, whether that site is hosted internally by the Department (or an operating unit) or an external commercial, academic, nonprofit, or other government agency, on behalf of the Department or an operating unit.

Department employees using SM/W2.0 technologies in an official capacity must do so only on Department-approved accounts and may only use official e-mail or other contact information for the creation and management of those accounts. In addition to helping the Department track how many accounts it possesses, using Department-approved accounts will ensure that the Department knows who is responsible for each account it uses. In the case of services that do not require accounts for the creation of a Department presence, employees should follow the service-specific guidance available on the Commerce Web Advisory Council's [Social Media Website](#).

In general, Department employees may only post from Department-approved accounts information that represents official agency positions (i.e., not personal opinion). However, if a posting concerns a fundamental research communication as defined by the Department's [Public Communications Policy](#) (DAO 219-1) and the posting is likely to be misinterpreted as an official Department position, Department employees must clearly state that they are providing their own personal opinions and not those of the operating unit, the Department, or the Federal Government.

Department employees should conduct themselves in a professional, courteous, and honest manner in all public communications about or related to their Government work, whether online, in person, at public meetings, or in other settings.

When posting a comment related to Department work to a public Web site, Department employees must identify themselves with their Department affiliation and/or official title.

Posted information should be accurate and factual. Although there is often a tradeoff between speed of communication and accuracy, employees speaking in an official capacity should take appropriate steps to ensure that the information that they provide is correct, and whenever feasible, to correct inaccurate information about Department work (especially on Department Web sites) that is brought to their attention.

All social media updates that are posted by Department employees, or written by Department employees for dissemination or use by an outside organization, must explicitly identify the Department as the source of the content. This requirement applies to all content authored by Federal employees and contractors of the Department. Examples of “outside organizations” may include cosponsors, stakeholder groups, media organizations, and SM/W2.0 sites. Further, when representing the Department online, Department employees must not engage in discussions of opinion about the Department’s programs; focus only on facts to avoid the perception that the Department is engaging in propaganda. Cite sources when providing facts.

Department employees may not post any unauthorized personally identifiable information on an SM/W2.0 Web site. Some PII may be subject to the [Privacy Act and may not be released unless consistent with the provisions of the Privacy Act](#). Questions concerning whether employees may release PII may be directed to the CPO or the operating unit Privacy Act Officer. The improper release of PII or other sensitive information may result in civil or criminal penalties.

Department employees may not improperly use or post materials protected by copyright, trademark, patent, trade secret, data rights, or related protections for intellectual property. Proper use may require obtaining written permission from the owner of such information. The Department’s Office of the General Counsel can assist employees in obtaining these permissions when necessary. Additionally, employees should exercise diligence with respect to the Department’s and their operating unit’s intellectual property, in logos, slogans, trademarked names, etc. Third-party use of Departmental emblems or logos requires pre-approval in accordance with [DAO 201-1](#), Approval and Use of Seals, Emblems, Insignia and Logos.

Department employees and operating units must not endorse commercial products or services. Department employees should not post commercial advertisements or otherwise engage in activities that might lead to a conflict of interest, appearance of endorsement, affiliation, or authorization, or otherwise lead the public to believe that your operating unit supports the views, products, services, etc. of third parties. (When considering demonstrating support for local/community efforts or organizations, please contact the Office of the General Counsel to ensure that support complies with relevant Department and ethics guidance.)

Department employees may not include surveys, polls, questionnaires, etc., on official SM/W2.0 Web sites unless the questions have received Office of Management and Budget (OMB) Paperwork Reduction Act clearance. The [Paperwork Reduction Act](#) (PRA) prohibits certain information collections by the Department without prior approval by OMB. While OMB has determined that some uses of social media are not considered information collection under the PRA, please contact the Office of the General Counsel to determine if the PRA applies to a specific use.

Department employees’ use of SM/W2.0 services must not include requests to contact a member of Congress, a jurisdiction, or an official of any Government (Federal, state, or local) to favor or oppose any legislation, law, or appropriation because these activities are prohibited by the Anti-Lobbying Act.

Department employees may not solicit consensus advice from the public using SM/W2.0 technologies. The [Federal Advisory Committee Act](#) prohibits agencies from receiving consensus advice from *de facto* committees or groups who are not made up entirely of Federal employees.

(2) Guidelines for Use of SM for Operating Units:

Department Web sites, pages, etc. that contain postings by an operating unit or the public require diligent monitoring.

Because monitoring and filtering of Department Web sites, pages, etc. may give rise to public criticism, operating units are required to use either the Office of the Secretary's [comment policy](#) or develop and post their own comment policy approved by the Office of the General Counsel. Operating units should post commenting guidelines prominently, when technically able to do so, and apprise public users of it regularly. Operating units using SM/W2.0 technologies must prevent the posting of or immediately delete postings by the public that contain:

- Comments regarding a political party or a candidate in a partisan political campaign (a campaign in which candidates are identified by political party);
- Requests to contact a Member of Congress or official of any government, to favor or oppose any legislation, law, or appropriation;
- Advertisements, endorsements, or promotions; and
- Vulgar or abusive language, personal attacks of any kind, or offensive terms targeting individuals or groups.

All social media updates that are posted by operating units, or written by operating units for dissemination or use by an outside organization, must explicitly identify the Department as the source of the content. This requirement applies to all content authored by Federal employees and contractors of the Department. Examples of "outside organizations" may include cosponsors, stakeholder groups, media organizations, and SM/W2.0 sites. Further, when representing the Department online, operating units must not engage in discussions of opinion about the Department's programs; focus only on facts to avoid the perception that the Department is engaging in propaganda. Cite sources when providing facts.

Operating units must ensure that the content maintained on their SM/W2.0 sponsors' Web sites, especially PII and other sensitive information, is secure and adequately safeguarded from unauthorized disclosure or destruction. The records must be retained consistent with the Department's [records retention requirements](#). NARA [Bulletin 2011-02](#), Guidance on Managing Records in Web 2.0/Social Media Platforms, provides additional guidance.

Operating units interacting with the public through SM/W2.0 technologies must ensure that such interactions require and generate the least amount of PII possible from their users. To that end, and whenever feasible, operating units must edit and actively manage their SM/W2.0 Web site or

application settings to make sure that only the minimum amount of PII necessary to effectively use such technologies is being generated/collected. OMB Memorandum M-10-23 establishes requirements for a PIA, which must document the agency's decision process. Agencies should discuss these details as appropriate in the privacy notice posted to the SM/W2.0 technology, as described in OMB Memorandum M-10-23.

Department Web sites must not collect any personal information from children (under the age of 13) in violation of the [Children's Online Privacy Protection Act](#).

When posting information using SM/W2.0 technologies, operating units should ensure and maximize the quality, objectivity, utility, and integrity of posted information (including statistical information), and ensure that measures are in place to allow for the correction of information not meeting that standard. This is required under the Department's [Information Quality Act Guidelines](#).

Operating units are required to ensure that people with disabilities or limited English proficiency have an accessible version of official content posted online, in compliance with [Section 508 of the Rehabilitation Act of 1973](#), and [Executive Order 13166](#), Improving Access to Services for Persons With Limited English Proficiency. Materials posted to SM/W2.0 services also must be posted in accessible formats on the official Department Web site; non-governmental SM/W2.0 sites may not be the sole location where content is posted. This will ensure that people with disabilities, or who have limited English proficiency, always have an accessible version of the content and that the official version of the content is located on a Department Web site.

If the SM/W2.0 technology allows the public to respond to official postings, the Department Web site also must provide visitors with the ability to communicate with the Department so that members of the public do not have to register with or provide personal information to third-party Web sites that may require registration or the provision of personal information. The Department Web site must provide an alternative way, e.g., e-mail address for members to communicate directly with the Department without providing personal information to a third-party Web site.

When visitors to an official Department Web site are redirected from the Department site to a third-party site, the visitors must be notified that they are leaving the official agency site, e.g., when a visitor to a Commerce site is redirected to view a video on YouTube®. The Department's notification should include an exit disclaimer stating that (1) the Department cannot attest to the accuracy of the information provided by a non-Federal Government site; (2) the link to the site is provided only for reference; and (3) the link to the site does not constitute endorsement of any product, service, organization, company, information provider, or content. Further, Department employees' use of links to such third-party sites must be consistent with their operating unit's linking policy. This is required by OMB Memorandum [M-05-04](#), Policies for Federal Agency Public Web Sites, and OMB Memorandum [M-10-23](#), Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010.

The Department may not rely on SM/Web 2.0 technologies as the exclusive means of distribution of information. Original materials posted to SM/W2.0 services also must be posted on official

Government Web sites, *and* alternative, non-electronic forms of information must be made available upon request, pursuant to OMB [Circular A-130](#), Management of Federal Information Resources.

(3) Hatch Act in the Workplace:

Department employees are prohibited by the [Hatch Act](#) from engaging in political activity on Government premises or using Government resources. Political activity includes any activity directed toward the success or failure of a political party or a candidate in a partisan political campaign. Thus, official use of social media may not include any reference relating to a political party, candidate, or campaign, including links to political websites or organizations.

Additional information is available from the OGC [Ethics Law and Programs Division](#) Web site, by phone at 202-482-5384, or via e-mail at ethicsdivision@doc.gov.

Applying for Official SM/W2.0 Accounts

Commerce employees should consult the list of Commerce approved [Social Media and Web 2.0 Web sites](#) and use the [Web-based Commerce Social Media Application](#) process (registration required) to apply for SM/W2.0 accounts. The process is overseen by the Office of the Secretary's Office of Digital Engagement, with input from operating unit's public affairs and chief information offices. The Office of General Counsel will be consulted as necessary.

General Guidelines for the Use of SM/W2.0 Technologies in an Unofficial Capacity:

The following are general guidelines for Department employees' unofficial or personal use of SM/W2.0 technologies. Please note that these guidelines for unofficial or personal use do not apply to Department contract employees, except to the extent that they are using Department resources to provide information to the public.

(1) Personal and Professional Communication:

Pursuant to the Department's [Public Communications Policy](#) (DAO 219-1), Department employees on Government or non-Government Web sites, who wish to post or upload original material that is not publicly available using SM/W2.0 technologies that relates to the programs or operations of their operating unit and that is related to their official duties, must submit their communication for review to their supervisor or a public affairs officer or other appropriate communications staff at their operating unit. A personal account must never be the first point of release for public documents.

Employees should be mindful of blurring their personal and professional life when using SM/W2.0 technologies. Employees should not establish relationships with working groups or affiliations that may reveal sensitive information about their job responsibilities.

Pursuant to section 7 of DAO 219-1 (Public Communications), researchers are free to participate in Fundamental Research Communications with the media and members of the public regarding their research in their unofficial capacity on personal social media accounts, but they are not required to do so. Given the nature of the scientific process, the role of the scientific community is to draw scientific conclusions based on available data. Department researchers may draw scientific conclusions based on research related to their jobs and communicate those conclusions to the public and the media in a Fundamental Research Communication. However, if such a conclusion could reasonably be construed as representing the view of the Department or an operating unit when it does not, then the researcher must make clear that he or she is presenting his or her individual conclusion and not the views of the Department or an operating unit.

Although Department employees are encouraged to learn about and experiment with these tools in an unofficial capacity, they should be mindful that any information posted on the Web, even when on-site privacy controls are used on SM/W2.0 sites, could become public.

Do not disclose any information obtained on the job that is not already publicly available. This includes national security (classified) information, personally identifiable information, proprietary or business confidential information, pre-decisional information, or similar sensitive information.¹

The Commerce [Internet Use Policy](#) allows employees to use their Government computer and SM/W2.0 for their personal use, provided that access is permitted by the operating unit CIO and use of equipment is minimal. Additionally, use of SM/W2.0 must not interfere with office operations or involve commercial activities (profit-making or business), partisan political activities, or sexually explicit communications.

(2) Employee Title Use:

You may use your title when it is self-evident that you are not posting in an official capacity, such as posting a resume or listing your employment history on a social network profile.

¹ This policy is consistent with and does not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this policy and are controlling.

Use of your job title in social media profiles must be considered within the totality of the circumstances to determine whether a reasonable person with knowledge of the relevant facts would conclude that the government sanctions or endorses your communication.

Relevant factors to consider in making the determination include:

- Whether you state that you are acting on behalf of the government;
- Whether you refer to your connection to the government as support for your statements;
- Whether you prominently feature your agency's name, seal, uniform or similar items on the social media account or in connection with specific social media activities;
- Whether you reference government employment, title, or position in areas other than those designated for biographical information;
- Whether you hold a highly visible position in the Government, such as a senior or political position, or are authorized to speak for the Government as part of your official duties;
- Whether other circumstances would lead a reasonable person to conclude that the government sanctions or endorses your social media activities; or
- Whether other circumstances would lead a reasonable person to conclude that the government does not sanction or endorse your social media activities.

Ordinarily, an employee is not required to post a disclaimer disavowing government sanction or endorsement on the employee's personal social media account. Where confusion or doubt is likely to arise regarding the personal nature of social media activities, you are encouraged to include a disclaimer clarifying that your social media communications reflect only your personal views and do not necessarily represent the views of your agency or the United States. A clear and conspicuous disclaimer will usually be sufficient to dispel any confusion that arises.

(3) Hatch Act on Personal Accounts:

The [Hatch Act](#) prohibits Federal employees from soliciting, accepting, or receiving campaign contributions, including through the use of SM/W2.0 technologies. This prohibition includes hosting or posting to a Web site that includes a link for making contributions to a political party or a candidate in a partisan election, that is, a campaign in which candidates are identified by political party.

Further, Department employees are prohibited by the [Hatch Act](#) from engaging in political activity on Government premises or using Government resources. This restriction includes using personal or Government devices for such purposes. Political activity includes any activity directed toward the success or failure of a political party or a candidate in a partisan political campaign.

Additional information is available from the OGC [Ethics Law and Programs Division](#) Web site, by phone at 202-482-5384, or via e-mail at ethicsdivision@doc.gov.

Other Applicable Commerce Policies

The use of SM/W2.0 services must conform to other applicable Commerce policies, including the following:

- Department's [Public Communications Policy](#) (DAO 219-1) , provides guidance for employees for communicating with the public about Commerce programs and activities and describes the role of the Office of Public Affairs (OPA) in ensuring that public communications are open and accurate, April 30, 2008.
- [Web Policies and Best Practices](#) developed by the Commerce Web Advisory Council and adopted by the Commerce CIO and Director of Public Affairs for implementation Commerce-wide, provide general guidance and requirements for the display of content on the Web.
- Commerce [Internet Use Policy](#), provides general guidance regarding Internet use by Department of Commerce personnel (employees, contractors, associates, and others) who are authorized to use Commerce resources, December 19, 2008.

Responsibilities of Chief Information Officers

Risk Assessment and Authorization for Use:

Before any SM/W2.0 service or technology is approved for use on any Commerce network or system, the responsible operating unit Chief Information Officer (CIO) must assess whether the users in the operating unit should be authorized to use or access a particular SM/W2.0 technology using established risk management methodologies. The relevant CIO should determine whether any risk-based limitations on access or usage by users within that operating unit are warranted prior to authorizing the use of a particular service or technology. The risk assessment should be conducted in accordance with the risk management principles in [NIST Special Publication 800-30 \(as amended\)](#), Guide for Conducting Risk Assessments, and other [NIST Publications](#) that apply. Additional guidance for CIOs is in the [Guidelines for Secure Use of Social Media by Federal Departments and Agencies](#).

A CIO's authorization to use a particular SM/W2.0 service or technology applies only to the operating unit for which the CIO is responsible. Depending on the level of IT security measures in place, a CIO may approve use of or access to a SM/W2.0 service on particular operating unit networks or systems but not others. Each CIO is responsible for maintaining a current inventory of SM/W2.0 technologies approved for access from their operating unit network(s) and systems.

Terms of Service and Privacy:

After assessing the risks, the relevant CIO must verify that the SM/W2.0 service provider terms of service agreement has been approved by the Department of Commerce, including the Department's Office of the General Counsel, before authorizing Commerce employee use of that service or technology. Approved service agreements are on the Commerce Web Advisory Council [Social Media Web site](#).

[OMB M-10-23](#) requires agencies to conduct a Privacy Impact Assessment (PIA) in all situations in which any personally identifiable information (PII) will become available to the agency. OMB M-10-23 also requires agencies to update agency privacy policies and post specialized privacy notices on the actual SM/Web 2.0 service itself, to the extent possible. Each responsible operating unit CIO must coordinate these activities with the Departmental Senior Agency Official for Privacy.

The Commerce CIO is responsible for oversight and monitoring of implementation of this policy by operating unit CIOs.

Specific IT Security Guidelines for Using SM/W2.0 Technologies

SM/W2.0 present IT security challenges beyond those of static Web sites, and it is essential to adhere to applicable Federal and Department IT security requirements, including the following:

- The Administrative Point of Contact (APOC) for a SM/W2.0 account is the individual who is solely responsible and accountable for the administration, password control, and access management of the account. An APOC may be anyone approved by the operating unit's Office of Public Affairs, Office of the Chief Information Officer and the Office of Digital Engagement through the Social Media Application process.
- APOCs should not use the same password for more than one account. Many SM/W2.0 sites allow account administrators to assign administrative rights to other users. When available, this feature should be used.
- APOCs must not use the same password for logging in to their Commerce or operating unit network that they use to access any SM/W2.0 site. Failure to use different passwords could compromise the security of the Commerce or operating unit network.
- APOCs should use two-factor authentication for all accounts where it is available and possible.
- Even in cases where SM/W2.0 Web sites do not enforce strong password requirements, strong passwords should be used in accordance with [CITR-009: Password Requirements](#) for password length, expiration, and complexity, e.g., use of upper and lower case letters and special characters.

- APOCs should assess and accept risk for accounts prior to putting content on a service and work with IT security community to complete a full risk assessment at the enterprise level. This is separate from accepting the Terms of Service.
- APOCs document areas where policy cannot be followed, e.g. using a government account to manage Facebook sites when Facebook does not allow individuals to have more than one account at a time.
- APOCs should only follow links and download files from known and secure sources. Any file downloaded from a SM/W2.0 site must be virus scanned before opening. Upon receipt of a suspicious message, link, or file to download from a known person, APOCs should verify that the item was actually sent by the person before virus scanning and opening it.
- SM/W2.0 accounts must be monitored on a regular basis. In the event pages are [hacked or defaced](#), a report must be sent immediately to [DoC Computer Incident Response Team \(CIRT\)](#) or the operating unit's IT Security Officer. After reporting the incident, the APOC for the account must contact the software or service provider to regain control of the account and restore the page. Passwords will be changed immediately after any hack or page defacement.

Resources for Additional Information

- Office of the General Counsel, [General Law Division](#), 202-482-5391.
- Office of the General Counsel, Ethics Law and Programs Division, 202-482-5384 or ethicsdivision@doc.gov).
- Office of the General Counsel, Employment and Labor Law Division, 202-482-5017
- Office of IT Policy and Planning, OCIO, 202-482-0275.
- Director of Digital Engagement, OSEC OPA, 202-482-3077
- Chief Privacy Officer and Director of Open Government, 202-482-3463
- Records Management Officer, OCIO, 202-482-4559

Data Stewardship Program

Use of Public Websites to Obtain Respondent Contact Information Policy

PURPOSE

This policy outlines requirements Census Bureau staff must follow when using public websites, including social media sites, to obtain contact information on a survey or census respondent.

BACKGROUND

Strict laws govern how the Census Bureau may collect information about households and establishments. Census Bureau staff collecting that information must obey those laws and act in ways that minimize respondent burden, while maintaining high response rates and efficiently using public funds. For all these reasons, these staff should use tools and technology appropriately to find out how best to contact respondents.

Public websites, including social media, have a rapidly growing role in American life. With the rise of mobile applications, Americans increasingly turn to them as a source of information replacing phone books, city directories, and trade guides. In addition, information from public websites including social media and information from traditional sources are seamlessly integrated in Internet search results. This vastly increases the likelihood Census Bureau staff will encounter all of these sources in the course of performing their tasks.

The Census Bureau has created this policy to provide guidance to its staff on using such public websites including social media in ways that respect respondents' privacy and preserve the public trust.

SCOPE

This policy applies to all field representatives and Census Bureau staff involved in data collection for obtaining respondent contact information. It applies to all demographic and establishment surveys and censuses.

For the purposes of this policy, "establishment survey or census" includes all surveys and censuses of businesses, non-profits, institutions, government units, and other organizations.

For the purposes of this policy "demographic survey or census" includes all surveys and censuses collecting information from individual persons and households. It includes special censuses and decennial operations.

For this policy, the term "website" includes mobile applications.

For this policy, a public website is defined as any website, including social media sites, that can be widely accessed through a public search engine (such as Google, Bing, and others) and without an account or logging into the site or a search engine. The information on these sites is readily available to any member of the public.

This policy does not cover the use of email. Staff corresponding with respondents via email must follow all Census Bureau policies regarding the use of email.

POLICY

Census Bureau field representatives and other staff involved in data collection must respect and protect the privacy of respondents and must uphold all legal requirements to keep that data confidential. To that end, field representatives and staff completing demographic and establishment surveys and censuses may need to obtain respondent contact information by searching public websites, including social media, but only in very limited ways.

Limited Use

During field data collection, Field Representatives and Census Bureau staff may use public websites and social media only to search for contact information on prospective respondents.

Staff should never be logged in to these websites when they use them. This ensures we only get contact information that respondents have made available to the public.

Staff may not use their Census Bureau email account to create a social media account.

On demographic surveys and censuses, field representatives and Census Bureau staff may only view information that a person has made publicly available. They may search only in contact information sections of public websites, including social media.

On establishment surveys and censuses, Census Bureau staff may use information from public websites including social media to verify or find the name of the person(s) whose position(s) at that establishment makes them the person likely to respond on behalf of their employer.

For the collection of data, field representatives and Census Bureau staff completing demographic and establishment surveys and censuses must follow all Census Bureau procedures specific to their assigned survey or census.

Guidelines for Using Contact Information

Field representatives and Census Bureau staff completing demographic and establishment surveys and censuses must **not** contact prospective respondents through public websites, including social media.

Field representatives and Census Bureau staff completing demographic surveys and censuses should not contact a prospective respondent at a work address nor at a work telephone number unless the respondent has given permission to do so.

Staff working on an establishment survey or census must follow the procedures of their census or survey when it comes to contacting a respondent.

Protecting Respondents' Information

Field representatives and Census Bureau staff collecting respondent data must protect any information gathered in the course of the survey or census. This includes information gathered from a public website including social media.

Appropriate protections include taking such measures as the field representative and Census Bureau staff clearing their browser and search histories after completing a search for a respondent's contact information.

EFFECTIVE DATE

This policy is effective upon signature.

LEGAL AUTHORITIES

Title 13 United States Code
Title 5 United States Code

IMPLEMENTATION

Individual program areas have responsibility for implementing this policy.

RELATED POLICIES

U.S. Department of Commerce, Policy on the Approval and Use of Social Media and Web 2.0, December 9, 2010

POLICY OWNER

Policy Coordination Office

SIGNATURE

By Direction:_____ Date:_____

Nancy A. Potok
Deputy Director and Chief Operating Officer

U.S. Census Bureau

Summary Information	
Policy Title:	Use of Public Websites to Obtain Respondent Contact Information Policy
Date Signed:	
Policy Owner:	Policy Coordination Office
Office Responsible for Implementation:	Program Areas
Office Responsible for Dissemination:	Policy Coordination Office
Stakeholder Vetting:	Vetted with ADEP, Decennial Directorate, FLD Headquarters, Philadelphia Regional Office, PCO, HRD, CNMP, CLMSO, PIO, the Legal Office, Respondent Advocate Offices of the Economic and Demographic Directorates



Department of Commerce

Commerce Information
Technology Requirement

CITR-021
September 21, 2012

Password Management

1. PURPOSE

This document establishes requirements for password authentication to DOC information systems, including their creation, protection, management, and administration.

2. BACKGROUND

Proper and secure authentication to systems is an essential pillar for an information security program that is built upon an effective defense in-depth approach. Authentication is a process that verifies the identity of an individual prior to granting access to a system, application, and/or data, including those that service the general public. This process relies on the ability of each individual to present unique identifiers (e.g., username and password). This key process then facilitates authorization and auditing, thereby controlling what information an individual can access, and recording when and where it is accessed within the infrastructure.

The key factors necessary for authentication to provide the desired protection are the uniqueness and the confidentiality of the identifying information. If authentication is compromised, then there are cascading effects that ripple through the infrastructure. This not only prevents proper authentication, but also diminishes the value of the authorization and auditing functions.

Weak passwords that do not conform to best practices are fertile ground for data and infrastructure breaches. It is every *user's* responsibility to closely safeguard passwords that meet the requirements set forth below.

3. SCOPE

This policy applies to employees, contractors, guest researchers, collaborators and others having access to and/or use of DOC information systems and applications, including third-party websites and applications used by DOC for DOC business purposes. Specifically, the requirements apply to DOC public access information systems; all DOC-owned computers; computers connected to DOC networks including computers connected to DOC visitor networks; and computers remotely connected to DOC networks (any access to a DOC network through a non-DOC controlled network, device or medium).

4. AUTHORITY

The DOC Chief Information Officer (CIO) has the authority to develop, implement, and manage information technology (IT) security processes and procedures to protect the availability, confidentiality, and integrity of the Department's IT resources. The DOC Chief Information Security Officer (CISO)/Senior Agency Information Security Officer (SAISO) shall ensure that IT security policy and requirements are developed consistent with applicable statutory authority, including the Clinger-Cohen Act and Federal Information Security Management Act (FISMA); with regulatory requirements and external guidance, including Office of Management and Budget (OMB) policy and Federal Information Processing Standards (FIPS) publications promulgated by the National Institute of Standards and Technology (NIST); and with internal policies and requirements.

5. CANCELLATION/AUGMENTATION OF EXISTING POLICY

This policy replaces *Appendix G: Password Management of the 2005 U.S. Department of Commerce IT Security Program Policy and Minimum Implementation Standards*, and *CITR-009, Password Requirements Version 1.1*.

6. GLOSSARY

Password -A secret, typically a character string, which a claimant uses to authenticate its identity.

Passphrase -A relatively long password consisting of a series of words, such as a phrase or full sentence.

7. POLICY

General Password Requirements

1. Passwords must be consistent with the following criteria:
 - a. Passwords for user accounts must have at least twelve (12) non-blank characters.
 - b. Passwords must contain characters from at least three (3) of the following four (4) categories:
 - i. English upper case characters (A ... Z);
 - ii. English lower case characters (a ... z);
 - iii. Base 10 digits (0 ... 9); and
 - iv. Non-alphanumeric characters (e.g., \$#%).
 - c. Passwords must not contain common words, nouns, pronouns, acronyms, contractions, and geographic locations (i.e., dictionary words).

Password Management Requirements

1. Passwords must be changed as follows:
 - a. At least every ninety (90) days;

- b. Immediately after being shared for emergency purposes;
 - c. Immediately if known or suspected to be compromised;
 - d. Immediately if discovered to be out of compliance with this standard; or
 - e. By direction from management.
- 2. If a determination is made that a password has been compromised or is not in compliance with this standard, but the password cannot be immediately changed, the account must be suspended until the password is changed.
- 3. Passwords must not be shared except in emergency circumstances or as specified in paragraph 7.3.
- 4. Passwords must not be reused for two (2) years, nor can any of the last eight (8) passwords used} be reused.
- 5. All vendor-supplied default passwords must be changed before the respective IT resource is connected to a DOC network.
- 6. If authorized access to critical systems would be prevented if the password were lost or forgotten, then the password must be documented and stored in a restricted, secure area (e.g., office safe with appropriate categorization level, locked file cabinet). Access to these passwords must be restricted to authorized personnel for purposes of maintenance and contingencies.
- 7. Passwords must be protected to prevent their unauthorized use. Passwords printed or written down must be protected from unauthorized access, as described in 7.2.6.
- 8. Passwords must be encrypted using a FIPS 140-2 validated cryptographic module when transmitted across the wide area network (WAN) and the Internet. Passwords should be encrypted using a FIPS 140-2 validated cryptographic module when transmitted across a local area network (LAN) in accordance with the Transmission Integrity (SC-8) and/or Transmission Confidentiality (SC-9) requirements of the system.
- 9. . Passwords must not be stored electronically in clear text or in any easily decipherable form.
- 10. Passwords must not be distributed through non-encrypted electronic mail and voice-mail. However, single use passwords (i.e., for password resets that must be changed upon first use) may be sent through non-encrypted electronic mail and voice-mail and must expire within 24 hours. If sent by regular mail or similar physical distribution system, passwords and user IDs must be sent separately.
- 11. User applications must not be enabled to retain or save passwords for subsequent reuse, or be configured to bypass authentication mechanisms. For example, Internet browsers must not be enabled to save passwords for reuse.

12. Use of password-retaining programs is allowed provided that access to the retaining program requires authentication and the program protects the storage of passwords.
13. Access to password files or password databases must be restricted to only those who are authorized to administer the IT system.
14. IT systems must be designed so that temporary user IDs, passwords, and parameters associated with other means of authentication automatically expire after a designated date.
15. System audit log should record failed login attempts} instances of changes to passwords, and the addition or modification of administrator/privileged accounts. After five (5) failed login attempts, the user must be disconnected from the service, and access suspended for at least five (5) minutes.

Group Password Requirements (i.e. single password used by more than one user):

1. May only be used when there is an overriding operational necessity as documented in an approved IT system security plan (SSP);
2. Must be used with some other mechanism such as access list control, personnel security or physical security, that can assure accountability;
3. Must be changed when any individual in the group is no longer authorized;
4. Must be different than passwords used to control general access on any given system;
5. Must not be shared outside the group of authorized users;
6. Must not be used for access to other applications;
7. Must never be re-used; and
8. Must comply with all other requirements in 7.1 and 7.2, except for 7.2.1 and 7.2.4

Public Application/System Requirements

DOC public applications and/or systems requiring passwords for access must employ the following requirements²:

1. Either passwords must have at least twelve (12) non-blank characters with no minimum password lifetime (i.e., expiration) OR passwords must have at least

² This section contains requirements for members of the public accessing DOC public-facing applications deemed to require passwords. OUs which have documented business cases for different requirements for public applications and/or systems used in support of mission critical public access may develop alternative, risk-based security requirements for those applications and/or systems.

eight (8) non-blank characters with a maximum password lifetime of no more than 90 days;

2. Address all other password criteria set forth in sections 7.1 and 7.2 above (with the exception of 7.2.1.a if no minimum password lifetime is needed per section 7.4.1);
3. Password resets must use pre-established challenge questions, or be reset manually by the application owner/administrator (i.e. via phone call with some type of identity verification);
4. Must include the ability for users to change their own password and post instructions for users to change their password if they believe it may be compromised;
5. The system must notify the user:
 - a. When their username or password has been changed;

When there have been five (5) or more sequential failed attempts to login to their account; and

- b. The time stamp of the user's last successful log into the system


Passphrase Management Requirements

1. Passphrases must have at least thirty (30) characters, including spaces.
2. Passphrases may be composed of multiple words (e.g., "These are the times that try mil).
3. Passphrases must follow requirements defined in 7.2.2 through 7.2.15.
4. Passphrases must be changed as follows:
 - a. Immediately after being shared for emergency purposes;
 - b. Immediately if compromised;
 - c. Immediately if discovered to be out of compliance with this standard; or
 - d. By direction from management.
5. Passphrase use must be documented in relevant system security plans.

8. Recommended Practices (not required by policy)

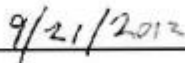
1. Try to create passwords that can be easily remembered. One way to do this is create a password based on a familiar phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmAyBelw@2R!" or "TmAyBE@IW>r-" or some other variation.
2. Passwords should not include any of the following:
 - a. Names of family, pets, friends, co-workers, fantasy characters, etc.;
 - b. Computer terms and names, commands, sites, companies, hardware, software;

- c. Birthdays and other personal information such as addresses and phone numbers;
- d. Word or number patterns like aaaabbbb, qwerty, zyxwvuts, 123321, etc.;
- e. Vendor-supplied default passwords;
- f. Control characters and non-printable characters (e.g., enter, or tab, or backspace, or ctrl-c, etc.);
- g. Any of the above spelled backwards; and
- h. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).



Simon Szykman

Chief Information Officer



Approval Date

Procedures for Reporting Unsolicited E-mail

Like many large organizations the Census Bureau receives a large number of unsolicited e-mail messages. The Bureau of the Census Computer Incident Response Team (BOC CIRT) as part of the Office of Information Security is the primary point of contact for employees who receive this type of e-mail traffic.

Reporting SPAM & Phishing E-mail SPAM E-Mail Awareness

Report SPAM and Phishing incidents by contacting the:

Census Service Center (Headquarters and Regional Office Staff)

- 301-763-3333, select Option 1 twice
- 1-877-343-2010, select Option 1 twice (24-hour support and toll-free)
- E-mail boc.cirt@census.gov (during business hours only)

Decennial Service Center (Decennial Field Staff)

- 1-855-236-2020, select Option 1 (24-hour support and toll-free)
- E-mail boc.cirt@census.gov (during business hours only)

Once BOC CIRT has received and triaged the incident, we will request e-mail headers and any applicable information such as details about attachments. Do not delete the message until instructed to do so by BOC CIRT. For instructions on extracting header information, see the section below.

SPAM E-Mail Awareness

- ☒ Never open attachments or URL links from unknown senders.
- ☒ Never open attachments or URL links with suspicious or potentially harmful names or file extensions (e.g., attachment.txt.vbs, attachment.exe) from known or unknown senders.
- ☐ Be suspicious of emails from known senders in which the subject line or content appears to be inappropriate for the existing relationship (e.g., an e-mail with the subject "I love you" from a professional colleague) or generic subjects (e.g., "Look at this, it's interesting").
- ☐ Never respond to spam e-mails.
- ☐ Never click an "Unsubscribe" button in spam e-mails.
- ☐ Scan all attachments with malware scanning software before opening, preferably by configuring the scanning software to automatically perform this task.
- ☒ Users will be warned about malware outbreaks and how to identify e-mails that might contain malware. These messages will be a BOC Broadcast message.
- ☒ If you have any questions as to the validity of an e-mail, report it as specified above and BOC CIRT will get back to you as soon as we have made a determination.

If you receive this type of message, follow the guidelines above for reporting this type of e-mail activity. BOC CIRT will request the appropriate information for action.

Phishing & Spear Phishing Instructions for extracting e-mail header information

What is Phishing?

Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing e-mails are crafted to appear as if they have been sent from a legitimate organization or known individual. These e-mails often attempt to entice users to click on a link that will take the user to a fraudulent website, or attempt to install malicious code. The user then may be prompted to provide personal information such as account usernames and passwords that can further expose them to future compromises. Additionally, these fraudulent websites may contain malicious code.

Learn More About Phishing

The following documents and websites can help you learn more about phishing and how to protect yourself against phishing attacks.

-  [Avoiding Social Engineering and Phishing Attacks](#)
-  [Protecting Your Privacy](#)
-  [Understanding Web Site Certificates](#)
-  [Anti-Phishing Working Group \(APWG\)](#)
-  [Federal Trade Commission, Identity Theft](#)
-  [Federal Trade Commission, Phishing Scams](#)
-  [Recognizing and Avoiding E-mail Scams \(pdf\)](#)

Instructions for extracting e-mail header information

When using Office 365 (O365) please extract the headers by following the procedure below:

1. Select/Highlight the unwanted e-mail
2. Right click the unwanted e-mail and scroll down to "View Message Details"
3. Select the Message Details containing e-mail header information
4. Copy the Message Details and close the window
5. Open the unwanted e-mail, click Forward from the Reply dropdown menu, and paste the Message Details in the forwarded e-mail

Note: Do not click on any links or open attachments in the opened, unwanted e-mail.

6. Send the header information to BOC.CIRT@census.gov

7. Delete the unwanted e-mail from your Inbox, Sent Items, Trash, and/or Deleted Items

Associate Director for Information Technology and Chief Information Officer (CIO)

Acceptable Use Policy for U.S. Census Bureau Information Technology Resources

PURPOSE

This acceptable use policy (AUP) governs the conduct of all Census Bureau personnel — Federal employees, contractors, associates, and interns — with access to information technology (IT) systems, regardless of method of access (government furnished equipment or personal device) or geographic location (i.e., local, virtual (VDI), or VPN). The AUP establishes the requirements of use for the Census Bureau network and the Internet using Census Bureau IT resources. This AUP communicates the role of Census Bureau personnel in protecting resources and data, as well as advises them of their obligations.

BACKGROUND AND AUTHORITY

To fulfill its mission, the Census Bureau collects and processes information from many sources; this information includes responses from individuals and businesses to surveys and censuses, administrative records from other agencies and personnel data. Federal laws such as Title 13, Title 26 and the Privacy Act (Title 5 section 552(a)) protect the confidentiality and privacy of this data and prohibit the unauthorized use of sensitive data by employees and contractors.

The Census Bureau encourages the mission-related use of the Internet as well as other government furnished equipment and resources, but allows limited personal use provided it does not violate any Federal laws, policies or regulations, interfere with official duties, pose a security risk, create the impression that the individual's personal views or activities represent the official position of the Census Bureau, consume excessive resources, or result in increased operations costs.

SCOPE

As representatives of the Census Bureau, all personnel — Federal employees, contractors, associates, and interns — will be held accountable for their actions and may be subject to criminal or administrative penalties, fines, termination, and/or imprisonment for any infringement of the agency's policy for IT systems use. By acknowledging receipt or using any Census Bureau IT resource, you are accepting responsibility for ensuring proper use and security of these resources. This policy covers all IT resources including workstations, laptops, tablets, mobile phones, RSA SecurID tokens, or other portable devices furnished by the government, as well as Internet services, including but not limited to, use of the World Wide Web, email, file transfer, remote computer access, news services, social networking or social media, instant messaging, blogs, wikis, file sharing sites, as well as streaming audio and video content.

POLICY

Official Work, Communications, and Access

Official Census Bureau work and communications must be carried out using an individually assigned Census Bureau account. Official communications are defined as any transfer of signs, writing, images, data, or intelligence for the intended purpose of supporting Census Bureau missions and objectives. Use of personal accounts for official work or communications is prohibited.

No one may access the Census Bureau enterprise or guest networks without authorization. Office-based personnel -- including headquarters, the National Processing Center and all current and future remote sites (including regional offices, contact centers, and decennial field offices) -- are mandated to use their enabled PIV (personal identity verification) card for access to the network in Census Bureau facilities in accordance with HSPD-12. Personnel not working in a Census Bureau facility -- field representatives, enumerators, teleworkers, remote access -- are required to use their username with password and RSA SecurID token for primary access to the network. Procedures are in place for individuals with lost or stolen PIV cards.

Work-Related Access

Census Bureau personnel are given access to Census Bureau resources based on the need to perform their job responsibilities. Census Bureau personnel are expected to work within the boundaries of this access and are not to attempt to access systems, applications, or data to which access has not been authorized. Census Bureau IT resources may be used to conduct mission-related work, in the administration and management of programs, censuses and surveys, and in the authorized dissemination of the results of Census Bureau work.

The criteria used in deciding acceptable use is based on general ethical principles of conduct, as well as government policies and statutory requirements. Specific criteria include defining whether the access and use is of benefit to the Census Bureau, whether it complies with government laws and regulations, whether access represents a potential security risk to information and IT resources, whether such access and use adversely affects others, and approval by appropriate Census Bureau management.

The policy against unauthorized browsing prohibits access to data, including non-sensitive information, for any reason other than work-related purposes. This means even if you can access information by having an active badge or elevated privilege log-on, you must not access the information unless you have a work-related need to do so.

The Census Bureau authorizes storage of non-Title data files in Office 365 (email, OneDrive, Sharepoint online). Title data (Title 5/13/26) should only be stored on approved Census network resources (e.g. M:\ drive, databases, AWS GovCloud, On-Prem Sharepoint). Specific conditions allow the use of Title 5/Title 13 data in Skype for Business meetings (please see Online Meetings section).

Internet storage/sharing of files through unapproved cloud-based services, personal email accounts, on-line storage, on-line backup, social media, or other sites to which files may be uploaded for sharing or storage is prohibited.

Remote management or support of an IT resource or application requires that only the specific screen for which the work is being performed may be displayed. Users should minimize all other applications on screen, such as email before granting access for remote IT support (e.g. from the Help desk).

Remote Access

Authorized teleworkers or authorized remote workers may view restricted data, such as Title 13, Title 26, Title 5, Personally Identifiable Information (PII), Business Identifiable Information (BII), confidential and/or other sensitive information only at their authorized alternative workplace or official duty station. Viewing restricted data at any other location or in a public place is prohibited. Only authorized employees may use Title 26 Federal Tax Information (FTI) while teleworking; contractors are prohibited from working remotely with Title 26 information. Further information and requirements may be found in the [Telework Policy](#) for Census Bureau employees, which contains the link to the employee [Telework Pledge](#), and the [Remote Access by Census Bureau-paid Contractors Policy](#), which contains the Contractor Remote Access Pledge.

All authorized teleworkers and authorized remote workers must have an up-to-date anti-virus program installed (such as McAfee or Norton) on their computer.

Privacy and Monitoring

Routine continuous monitoring of network and IT systems is conducted to identify and respond to performance-degrading events such as equipment failures, capacity issues, security threats, and security breaches. Therefore, all employees, contractors, associates, and interns using Census Bureau IT systems should be aware that information transmitted by or stored on IT systems within the Census Bureau's purview is not private and may be revealed during the course of routine monitoring.

Anyone using Census Bureau provided IT resources for official or personal use consents to such monitoring. If monitoring reveals evidence of possible misconduct or criminal activity, such evidence of the activity will be referred to the appropriate officials for appropriate action, including further referral to law enforcement as necessary. Users are reminded that use of Census Bureau's email, Internet, or IT resources for personal activities is subject to monitoring and therefore cannot be considered private.

Security Practices

Census Bureau personnel are responsible for securing their IT resources (i.e., workstations, laptops, virtual desktop, tablets, mobile phones, etc.) to prohibit unauthorized access. Census Bureau personnel shall:

- Log out of a secure application when the application is no longer in use
- Remove PIV card from card reader, lock their workstation, log out of the session, or use an authentication protected screen saver when leaving their workstation unattended

- Log out of VDI or Virtual Private Network (VPN) session and power off their Census Bureau workstation at the end of each workday
- Not share network, workstation, or device passwords with anyone except authorized Census Bureau personnel such as IT Help Desk staff. Once shared, passwords must be changed as soon as possible after the need has ended. If there is a chance a user's password has been compromised, it must be changed immediately
- Be careful while typing a password or PIN so that the password or PIN is not observed
- Ensure the workstation, laptop, or mobile device is not accessed by unauthorized persons
- Report suspected unauthorized IT resource access to the Census Service Center on 301-763-3333 or 1-877-343-2010, select Option 1 twice. Decennial Field staff should contact the Decennial Service Center on 1-855-236-2020, select Option 1.

Data Backup

Work related files should not be stored on any workstation's or laptop's hard drive (the C:\ drive). Store files either on your network home directory (the H:\ drive), network shared directory (the M:\ drive), SharePoint/OneDrive, or your area's document management system. Only files stored on network directories and server shares are backed up. There is no recovery of files stored on your workstation or laptop such as when your workstation or laptop is compromised by malware. No files or applications are backed up on mobile devices.

Software Use

Census Bureau staff may install authorized software on their assigned equipment that has been made available to them via the Software Center SCCM. Software, cloud services, web services, or any other offering or product that has been submitted and approved by [the Standards Working Group \(SWG\)](#), prior to the lifecycle end date, and scoped for use by a user, branch, division, etc., is considered authorized. Copyrighted software must be installed consistent with the respective licensing agreement and only after the installation has been approved by Census Bureau management. Installing software that is not explicitly authorized by the SWG or available in the Software Center SCCM is prohibited. **Personally owned software, or any software (including screensavers) that has not been approved by the SWG, is prohibited from being installed on Census Bureau equipment and shall be removed.**

The [Software Asset Management \(SAM\) Policy](#) establishes the authority, objectives, and mechanisms for managing, controlling, and protecting the U.S. Census Bureau's software assets throughout their lifecycle. This Policy applies to all processes and policies utilized in the acquisition and management of software resources regardless of their location in the Information Technology (IT) environment.

The intent of the SAM Policy is to facilitate effective mitigation of software security vulnerabilities, achieve cost savings, identify customer software needs, and ensure compliance with numerous federal directives via strategic software lifecycle management.

Census Bureau IT Equipment Use

Use of Census Bureau workstations, laptops, mobile devices, wired or wireless communications systems, data and other information is meant for authorized purposes only.

- All Census Bureau owned and furnished equipment must be protected and used appropriately and efficiently without waste and abuse.
- If you do not need or do not use a Census Bureau device for business purposes, the device shall be returned. All unused IT equipment returned must be stored in an authorized storage area, not remain on a desk or in a cubicle. Devices that are not in use and that are not returned will be disabled and may be reported as lost, stolen, or missing.
- If you have a Field Representative or enumerator device, do not allow anyone who is not a Census Bureau employee to use your device (unless it is required as part of the survey process, such as using a laptop for Audio-CASI).
- Do not leave your laptop or other mobile device in a vehicle, even for a short period of time. If you must do so, put it in the trunk of the vehicle. If the trunk is not accessible, make sure the laptop is not visible from the windows of your vehicle. Make sure the windows are up and all doors are locked.
- Requests to move Census Bureau IT equipment may only be completed by the authorized Office of the Chief Information Officer OCIO staff.
- All Census Bureau IT equipment must be identified within a [System Security Plan \(SSP\)](#) and must be managed/maintained in accordance with all applicable laws and regulations.
- OCIO reserves the right to disable, retrieve, or otherwise remove any Census Bureau IT device based on failure to meet compliance requirements, or for any identified risks to the Census Bureau environment.

Unacceptable IT Resource Use

Census Bureau personnel are expected to conduct themselves professionally in the workplace and refrain from using IT resources for activities that are inappropriate. Unauthorized use of Census Bureau equipment is prohibited. Unacceptable and prohibited uses of the Census Bureau Internet access, systems, and networks include, but are not limited to:

- The engagement in any activity, which would bring discredit upon the Census Bureau or the Federal government, or which would violate any statute or regulation or policy
- The engagement in any activity, which might cause congestion, delay, or disruption of service to the legitimate business related activities (e.g., streaming of video, audio files or sending of large file attachments, which could degrade network and Internet performance)
- The use of personal accounts for Census Bureau related business activities
- The use of official Census Bureau accounts for personal activities
- The use of peer-to-peer file sharing sites and services, e.g. Dropbox, Teamviewer, and Box, Inc. The use of instant messaging services, to include those packaged with social media sites, not approved for work-related activities, unless offered as a centralized shared service for the organization.
- The use of official titles, office and email addresses in personal communications, creating the impression the activity is sanctioned by the Census Bureau
- The use of official titles, office, and email addresses to register at websites, not related to Census Bureau business activities
- The use of official titles, office and email addresses to voice personal opinions and personal beliefs in conflict with the Census Bureau position
- The use of applications in an attempt to bypass Census Bureau security controls, when accessing the internet. Please contact the [SWG](#) or [OIS](#) for more information.
- The use of Census Bureau resources in the pursuit of "commercial business activities"

- The use of Census Bureau resources in the pursuit of "for profit" ventures
- The use of Census Bureau resources to support the success or failure of a political party, candidate for partisan political office, or partisan political group, or activity in support of political fund raising
- The intentional creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually-oriented material or materials that might be offensive to others
- The intentional creation, downloading, viewing, storage, copying, or transmission of explicit content involving children
- Performing searches for explicit sexual content of any type from devices connected to the Census Bureau network
- The intentional creation, downloading, viewing, storage, copying or transmission of materials related to gambling, illegal weapons, terrorist activities, and any other illegal or otherwise prohibited activities
- The intentional creation, downloading, viewing, storage, copying, or transmission of sensitive or classified materials (e.g. WikiLeaks, Pastebin) which have not been cleared for public release through the appropriate channels.
- The intentional use of government resources to acquire (download), store, share, reproduce or distribute copyrighted materials in violation of copyright laws (e.g. music, video, audio, or books)
- The intentional acquisition, use, installation, reproduction, transmission, or distribution of unapproved/unauthorized software for use on Census Bureau IT resources
- The dissemination of non-public information to external parties, newsgroups, bulletin boards or other public forums without authority
- The use of Census Bureau IT resources to participate in, or encourage others to participate in illegal activities or the intentional creation, downloading, viewing, storage, copying, or transmission of materials that are illegal, offensive or discriminatory
- The use of Census Bureau IT resources to access other networks or systems in a manner that violates Federal law or the policies of the owner
- The transmission of sensitive information without adequate security protection or authorization
- The use of an individual's title or the name of a Census Bureau office when using a social networking site, blog, wiki, video or other file sharing site, or other Web site or Web service for personal reasons
- Texting, browsing, using applications, as well as sending or receiving phone calls with a mobile device while operating any type of motor vehicle, unless the device is "hands-free" and allowed by law
- Transfer of work-related information to unauthorized devices.

Census Bureau Mobile Device Use

Mobile devices include, but are not limited to, smartphones, cell phones, tablets, laptops, and other devices that use cellular and broadband communications. Use of equipment will be periodically reviewed to ensure compliance with this policy.

- Minimize the use of mobile devices to reduce the cost of mobile devices and cellular plans
- Only use functions that are enabled on mobile devices; do not attempt to enable other functions. The Census Bureau will provide approved business-related applications

- Mobile devices may be disabled and wiped at any time, when deemed necessary, without regard to applications or data that you may have purchased and downloaded
- The Census Bureau reserves the right to enable or disable specific capabilities such as location services, camera, etc. on Government-issued mobile devices to aid in inventory, security functions, and, location of lost or stolen equipment.

Limited Personal Access and Use

The Census Bureau permits limited personal use of its IT resources including the Internet, provided such access and use is not illegal, does not interfere with job performance or official business, does not present a security risk to Census Bureau systems or data, does not consume excessive resources or network bandwidth, or discredit the Census Bureau. Limited personal access and use is a privilege and may be revoked at any time when deemed appropriate by Census Bureau management.

Excessive use of IT resources includes, but is not limited to, activities such as: filling an email box with personal messages; creating or transmitting personal mass mailings or chain letters; creating, uploading, downloading, sending large personal files via the internet (personal email accounts, social media, on-line storage and/or file sharing sites); as well as downloading or streaming audio or video content.

The Census Bureau-issued Field Representative or enumerator device may be connected to the Internet and only to conduct official Census Bureau work. Typical acceptable use includes transmitting Computer Assisted Personal Interviewing (CAPI) work and payroll information, as well as browsing approved internet sites. In addition, a remote connection by authorized Census Bureau personnel for troubleshooting purposes is appropriate.

Foreign Travel

Census Bureau employees on overseas assignments must obtain international travel agreements (ITA) and must be issued special Government-Furnished Equipment (GFE) from a loaner pool of devices specifically authorized for foreign travel. Individuals are not authorized to use any personal equipment to connect to the Census Bureau's network, including VDI, from anywhere outside of the United States or its territories. This includes connecting through the use of anonymizers, or third-party virtual private networks (VPN). Individuals are also prohibited from using their Enterprise operational information technology computing device (phone, laptop, tablet, etc.) in a foreign country.

The U.S. Census Bureau policy on the "[Use of Government-issued Information Technology Client Computing Devices on Foreign Travel](#)" provides details on the use of Census IT resources on foreign travel.

Email Use

Census Bureau personnel should take into consideration the following when utilizing the email system (either through provided workstation software or via remote access):

- All messages sent using Census Bureau email and communications systems are the property of the Census Bureau

- Do not send sensitive PII or BII or other sensitive administrative information of any kind in the body of an email. Instead, all sensitive information must be encrypted using a Census Bureau-approved encryption solution such as Kiteworks, and sent as an attachment. [Note: Kiteworks automatically encrypts attachments and not the body of the message.]
- Do not send illegal transmissions; you must adhere to copyright laws
- Do not open email messages or attachments if you are uncertain of the content or the sender
- Report suspicious emails to the Census Service Center on 301-763-3333 or 1-877-343-2010, select Option 1 twice. Decennial Field staff should contact the Decennial Service Center on 1-855-236-2020, select Option 1. You may also forward the email to boc.cirt@census.gov during business hours only.

Data loss prevention technology is used to detect and quarantine unencrypted outbound email messages and attachments to detect inappropriate transport of sensitive information. Additionally, inbound email messages containing sensitive information, while not quarantined, are tagged so that the recipient is notified of the information and to mitigate possible re-transmission of the information. Examples of sensitive information include the following: health information, Social Security Numbers, Tax Identification Numbers, and credit card information, even if it is your personal information. Such information is prohibited by Federal policy from unencrypted email transmission.

Email auto-forwarding of any kind from your Census Bureau email is prohibited. Auto-forwarding creates the potential for a serious operational risk, and risks unintentional disclosure of information, sensitive or otherwise. Auto-replies or out-of-office settings are permitted. Auto-replies are usually used when staff is out of the office or on vacation to notify people of their absence.

Personal/Non-Census Bureau IT Equipment Use

Personally owned or Non-Census Bureau -issued computers, laptops, tablets, smartphones, etc., are prohibited from direct connection to the Census Bureau enterprise network. Individuals may use personally owned or Non-Census Bureau-issued devices to access the Census Bureau VDI, authenticating with their username, password, and approved two-factor authentication such as PIV/PIN or RSA SecurID token. Individuals may use personally owned or Non-Census Bureau-issued devices to access the Employee Wireless network (System-11), authenticating with their username and password. Visitors of the Census Bureau must go through a registration process with their sponsor before obtaining access to the Guest Wireless network (System-10). A username and password will be provided for short-term use. Individuals are prohibited from connecting any unauthorized personally owned/Non-Census Bureau-issued devices to Census Bureau IT equipment.

Online Meetings

For Census Bureau hosted online meetings, users are approved to use Skype for Business and Census Bureau provided WebEx (census.webex.com):

- Skype for Business (SFB) allows the use of Title 13, Title 5, and PII during online meetings with some restrictions. Attendees must be Census Bureau employees and Special Sworn Status individuals who are authorized and have a business need to access the data. Title 26, Pre-Release Indicators and Embargoed data are NOT permitted. Please see guidance on

using [Skype for Business with Title 13 Data and Sensitive PII](#) for more information.

- For online meetings using WebEx, the use of Title 13, Title 5, Title 26, PII, or BII is prohibited. By attending a Census Bureau-approved WebEx online meeting, training, or event, you agree to abide by this policy. There is no right to privacy for data used in presentation, stored on, or accessed during web conferences. The Census Bureau reserves the right to delete web conferencing data in accordance with this and other Census Bureau policies.

For online meetings not hosted by the Census Bureau:

- The use of sensitive data such as Title 13, Title 5, Title 26, PII or BII is prohibited.
- When attending an online meeting not hosted by the Census Bureau, users cannot give remote control to an external meeting participant.
- Only secure meeting services shall be used. Online meeting services that allow insecure protocols such as SSLv3 or TLSv1.0 are not authorized for Census business use.

For situations not listed here, please contact the Policy Coordination Office (PCO) for further guidance.

IT Security Incident Reporting

Census Bureau personnel are required to promptly report incidents involving information, equipment and IT resources. Incidents may include suspected or confirmed presence of malware, policy violations, misuse, loss or breach of PII or BII, loss of a two-factor authentication device (such as an RSA SecurID token), etc. Further, personnel may not impede actions to conduct a forensic evaluation and/or sanitize IT resources. To reduce risk and liability to the Census Bureau, incidents shall be reported as soon as they are observed or reported to them. Actual or suspected loss of sensitive data must be reported within one hour of discovery.

- If you are aware of an IT security incident, contact the Census Service Center on 301-763-3333 or 1-877-343-2010, select Option 1 twice.
- Decennial Field staff should contact the Decennial Service Center on 1-855-236-2020, select Option 1.
- You may also forward suspicious emails to boc.cirt@census.gov during business hours only.

PRIVILEGE REQUIRES ADDITIONAL AUTHORIZATION AND APPROVAL

User Granted Developer or Support-Elevated System Privilege to Workstation or Laptop

Any user who is granted elevated IT system privileges, either in a support or developer role, is prohibited from performing the following:

- Download or install applications software, patches, or updates for existing software packages from the Internet or other media to a workstation or laptop

- Adding or installing personally-owned hardware to your workstation such as cell phones, digital cameras, USB Flash drives, and RAM
- Add, modify or delete security policies on the workstation
- Add, modify, or delete registry entries unless it is directly related to software you are developing
- Disable, modify, or delete any software icons that appear in the taskbar
- Remove any software using the Control Panel add/remove programs feature
- Delete any Windows operating system updates or security patches deployed to your workstation
- Modify the security, privacy, or advanced options for any of the Internet browsers
- Change the computer name or domain membership
- Add, start, or stop services on the workstation
- Add, modify, or delete any of the settings under the security, user account, or the network connections options
- Make any system configuration changes that have not been submitted through the appropriate change management process

User Initiated Daily Restart for Workstation Access with Non-Shutdown Waiver

Individuals with an authorized business need, such as system administration support and developers, may require an application or connection to continue processing overnight without a shutdown. Upon request through Remedy Service Request Management (SRM), an individual may be allowed to restart their workstation at a time of their choosing so that the reboot does not interfere with application processing. The reboot protects the network and IT systems by updating the workstation with software and operating system patches. Any person who is approved to receive exemption from shutdown is required to reboot their workstation daily; otherwise, an automatic reboot will be forced on the system.

User Granted Elevated System Privileges to Microsoft Windows Servers (Elevated Access and Service Accounts), Separate Acknowledgment Form Approved in Remedy SRM Process

Census Bureau personnel with elevated privilege to Windows servers shall be issued two accounts:

- A non-privileged, general use account that will allow internet use
- An authorized elevated privileges account that will restrict internet usage

A user with two separate accounts must use their enabled PIV card for primary network access and will be required to log on and log off to each account in order to gain access to required resources. Any user approved to receive an elevated privilege account is required to use that account to log into pertinent server systems. Use of the general use account (the JBID) is prohibited. Service accounts should be integrated as needed into installations and should not be used to log into servers.

Users are also prohibited from implementing changes or performing the following, without abiding by the established change control process or emergency procedures as outlined in the IT Windows System Service Level Agreement:

- Rebooting the server

- Downloading or installing unapproved applications software, patches or updates for existing software packages from the internet or removable media
- Adding, modifying or deleting registry entries
- Disabling, modifying or deleting any software icons within the taskbar
- Removing any software located in the control panel's add/remove programs feature
- Adding, starting or stopping services
- Create local accounts

Users are prohibited from the following under any conditions:

- Deleting any Windows operating system updates or security patches deployed to the server
- Adding, modifying or deleting security policies on the server
- Adding or installing personally-owned hardware to the server such as cell phones, digital cameras, USB Flash drives, etc.
- Modifying the security, privacy, or advanced options for any of the internet browsers
- Changing the server name or domain membership
- Adding, modifying or deleting any of the settings under the security, user account or network connections options
- Disclosing account information including passwords to another co-worker
- Logging on to any other server that you are not authorized to access with your account credentials
- Logging on to any system using someone else's account credentials whether you are authorized access or not
- Making any system configuration changes that have not been submitted through the appropriate change management or emergency processes
- Incorporating elevated privilege account IDs or passwords into scripts or any programming routines

User Granted Elevated System Privileges for Linux Servers

[Sudo Access Policy for Linux](#)

Access Types

In accordance with published policies and standards, the Computer Services Division (CSvD) has the authority to grant Sudo access. Two types of access are available:

Role	Account Type	Duration
Application Manager	Command Access, Service Account Access	As determined by CSvD
System User	Service Account Access	As determined by CSvD

Command Access provides individual commands required for specific tasks and a limited set of predefined collections of commands, e.g. the file manipulation commands include mv, cp, rm, chown and chmod.

Service Account Access provides access to service accounts or service account commands that are not a risk to system security.

The following types of access are not permitted:

- Sudo to root
- Scripts that allow root access
- Commands with known vulnerabilities that allow access to a root shell
- Commands that may compromise the security of a system

CSvD will remove Sudo access found to be in violation of published policies and standards.

Request Process

Application Managers and System Users may request access by submitting a Remedy ticket to CSvD that includes the type of access being requested and a business justification that clearly states the reason(s) Sudo access is required. CSvD Management and Security personnel review access requests on a case-by-case basis and notify requestors of the outcome within five business days of receiving a request.

Separation of Duties

- CSvD administrators propose and implement the Sudo changes.
- CSvD Security review violation citations, changes to the Sudo files and proposed changes.
- CSvD Management approve the changes that were proposed and approved by security.

IMPLEMENTATION

All Census Bureau staff are required to review and accept the Acceptable Use Policy (AUP) prior to receiving network access and yearly thereafter. New employees in Headquarters and the National Processing Center will sign the AUP acknowledgement during new employee orientation. Contractors, Field staff, and Regional Office staff acknowledge acceptance by clicking on the "I Accept" button after opening and reading the AUP in the Data Stewardship and IT Security Awareness Training prior to onboarding. For continued access to IT resources, all staff and contractors must annually accept acknowledgement of the AUP when they complete the mandatory Data Stewardship and IT Security Awareness Training. This process must be completed before July 1 or their network access will be terminated.

ENFORCEMENT

Unacceptable access to, or use of, Census Bureau information and IT resources is punishable by penalties. Individuals engaging in unacceptable or inappropriate access or use shall also be subject to having all access credentials indefinitely suspended at the discretion of Census Bureau management or Chief Information Officer.

LEGAL AUTHORITIES

- 5 CFR 2635 – Standards of Ethical Conduct for Employees of the Executive Branch
- 41 CFR 101-35. 201 - Telecommunications Management Policy
- Title 5 U.S.C. 552a – Privacy Act
- Title 13 U.S.C. 9 – Census - Confidentiality
- Title 18 U.S.C. 2510 - The Electronic Communications Privacy Act
- Title 18 U.S.C. 1030 - Computer Fraud and Abuse Act
- Title 26 U.S.C. – Internal Revenue Code
- Title 31 U.S.C. § 1301 – Use of Appropriated Funds
- Title 50 U.S.C. 1809 -Chapter 36 - Foreign Intelligence Surveillance
- Title 50 USC Chapter 36, Subchapter I - Electronic Surveillance
- Executive Order 12674 – Standards of Ethical Conduct for Employees of the Executive Branch
- Executive Order 13513, Federal Leadership on Reducing Text Messaging While Driving, October 1, 2009
- Census Bureau IT Security Program Policy (ITSP)

RELATED DOCUMENTS

[Census Bureau IT Security Program Policy, Version 6.2](#)

[2017 Required Security Controls for Census Bureau Information Systems](#)

[U.S. Census Bureau Telework Policy, 2019](#)

[Remote Access for Census Bureau-paid Contractors Policy \(including Remote Access Pledge for Census Bureau-paid Contractors\)](#)

[Census Bureau Safeguarding and Managing Information Policy \(DS007\), May 2013](#)

[Census Bureau Data Breach Policy \(DS022\)](#)

[DS017 Data Stewardship Awareness Training Policy, 2017](#)

[Ethics Rules, United States Department of Commerce, Office of the General Counsel, Ethics Law and Programs Division, 2016](#)

[Annex 8: Access and Use Policy, 2019 Department of Commerce Information Technology Security Baseline Policy, DoC Office of the Chief Information Officer, 2019](#)

[Census Bureau Control of Access to Personally Identified Survey and Decennial Census Data: Unauthorized Browsing Policy \(DS018\), March 2009](#)

[Privacy Policy, United States Department of Commerce, 2008](#)

[OMB Memorandum M-04-26, Personal Use Policies and “File Sharing” Technology, Office of Management and Budget, 2004](#)

[Department Administrative Order 202-751: Discipline, United States Department of Commerce, 1980](#)

EFFECTIVE DATE


The policy will become effective upon signature by the authorizing official.

POLICY OWNER

The Associate Director for Information Technology and Chief Information Officer owns this policy.

The chiefs of the Office of Information Security (OIS), LAN Technology Support Office (LTSO), Telecommunications Office (TCO), Computer Services Division (CSvD) and Policy Coordination Office (PCO) are responsible for maintaining, implementing, and disseminating this policy.

SIGNATURE



Kevin Smith
Associate Director for Information Technology and Chief Information Officer

9/27/19

Date

Summary Information	
Policy Title	Acceptable Use Policy for U.S. Census Bureau Information Technology Resources
Policy Owner	Information Technology Directorate
Office Responsible for Implementation	LTSO, OIS, PCO, TCO, CSVD
Office Responsible for Dissemination	LTSO, OIS, PCO, TCO, CSVD
Stakeholder Vetting	LTSO, OIS, PCO, TCO, CSVD

Version Information	
September 26, 2013	CIO signed AUP for FY14 Data Stewardship
March 2014	AUP expanded to include Internet Use Policy
September 2015	Annual review and update of AUP
September 2016	Annual review and update of AUP
September 2017	Annual review and update of AUP
September 2018	Annual review and update of AUP

Version Information	
September 2019	Annual review and update of AUP

If your acknowledgement and acceptance of the Acceptable Use Policy (AUP) for Information Technology Resources is not recorded electronically, please complete and sign below showing your acceptance of the AUP.

Acknowledgement and Acceptance of the Acceptable Use Policy for U.S. Census Bureau Information Technology Resources, September 2019

NAME: _____
Please print.

USER ID: _____
(User ID assigned after start date)

SIGNATURE: _____

DATE: _____

Glossary

Acceptable Use Policy

Provides guidance that applies to personnel who have authorization to use Census Bureau computer resources and have the ability to access the Internet from a government owned computer. The policy applies to computer use in Census Bureau facilities and in remote locations.

Administrative Records

Microdata records contained in files collected and maintained by other administrative or program agencies and commercial entities. They provide information about specific individuals and businesses, as well as regional, state, and local governments.

Administratively Restricted Information

Consists of agency documentation that is not intended as a public information product. This may include such things as contractor proprietary information, pre-release data, budget information, or pre-published research papers. May also include Personally Identifiable Information (PII).

Backdoor

A tool installed by a cyber-criminal to allow an attacker to circumvent any security measures in a computer system.

Bureau of Census Computer Incident Response Team (BOC CIRT)

The entity responsible for handling reports of confirmed or suspected data breaches.

Business Identifiable Information (BII)

Data collected or acquired for statistical purposes about a business that is maintained by Census Bureau or other Federal or state agencies, including, but not limited to business name, address, NAICS code, number of employees, payroll, sales, assets, and other financial data that could be used to identify individuals, businesses, and other organizations.

Computer Security Incident

NIST SP 800-61 defines a computer incident within the federal government as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.

Confidential Information Protection and Statistical Efficiency Act (CIPSEA)

A law that provides rules governing some surveys that the Census Bureau performs for other agencies.

CIPSEA provides strong confidentiality protections for statistical information collections, such as surveys and censuses, as well as for other statistical activities, that are sponsored or conducted by Federal agencies. It also requires a work related “need to know” in order to access protected data.

Confidentiality

An aspect of Data Stewardship that concerns protecting identifiable information from unauthorized disclosure. Confidentiality relates to how we protect information after we collect it.

Countermeasure

A response to a threat or vulnerability. Information security countermeasures can be actions, devices, procedures and techniques. Password rules and password-protected screen savers are examples of countermeasures that help protect sensitive information and resources from unauthorized access.

Cyber-Criminal

A person who actively tries to take advantage of vulnerabilities in a computer system to gain unauthorized access to sensitive information. The goals that a cyber-criminal may have are numerous. Cyber-criminals may try to retrieve information for their own personal use and may also try to disrupt the system and alter the data.

Data Breach

A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any other circumstance in which people other than authorized users, and for an authorized purpose, have access or potential access to personally identifiable information or business identifiable information in a usable form, whether physical or electronic.

Data Steward

All Census Bureau employees, contractors, and other individuals with Special Sworn Status are Data Stewards.

Data Stewards are responsible for adhering to all regulatory requirements and internal data policies and standards. This includes fully meeting the legal and reporting obligations levied by the Census Act, the Privacy Act, and other applicable statutes, including the requirements of governmental and other suppliers of data to the Census Bureau. Data Stewards are responsible for following all security controls mandated by the Census Bureau.

Data Stewardship

The formal, continual process we use to care for the information that is entrusted to us. This can be information we collect, information we receive, information we release, and information about our employees.

Disclosure Review Board

Census Bureau's Disclosure Review Board assesses data products prior to release to ensure they meet all of the disclosure avoidance requirements.

E-Government Act

A law that requires specific attention to privacy. For example, this law requires federal agencies to conduct Privacy Impact Assessments (PIAs) prior to developing or procuring information technology systems that handle personal information.

Encryption

This is the process of converting plain text or data into a form that cannot be read without decrypting or deciphering.

Federal Desktop Core Configuration (FDCC)

The standard desktop configuration mandated by the Office of Management and Budget (OMB).

Federal Information Security Act (FISMA)

One of the laws that protect information systems. Part of the E-Government Act. Under FISMA, federal agencies must provide security for the information and information systems that they manage. FISMA also defines the security measures that agencies must have in place for an effective information security program.

Federal Tax Information (FTI)

All data about businesses or people the Census Bureau receives from the IRS. Census Bureau projects using FTI are subject to the confidentiality provisions of the Internal Revenue Code — Title 26, U.S.C., as well as those of the Census Bureau Title 13, U.S.C. The confidentiality of FTI provided to the Census Bureau is perpetual – it does not end after a set number of years.

File Transfer Protocol (FTP)

A method of adding or removing electronic files to or from locations on the Internet.

Firewall

An information technology feature that provides a level of protection to computer systems by managing the electronic traffic to and from the system. The goal is to allow authorized traffic to pass through and to block unauthorized traffic.

For Official Use Only

This category identifies information that is exempt from mandatory release under the provisions of the Freedom of Information Act (FOIA). This information might include operational documentation such as contracting information (contracts, proposals,

evaluations), employment testing materials, budget proposals, security procedures, lock-up data (economic indicators) and other materials of a similarly sensitive nature that could be protected under the FOIA. “For Official Use Only” (FOUO) is not a security classification, it is simply applied to the kinds of materials noted above as a cautionary alert to warn that the documents might be protected under the FOIA. If the materials do not appear to be protected by the FOIA, do NOT mark them “For Official Use Only.”

Freedom of Information Act (FOIA) (5 U.S.C. 552)

A law that generally provides that any person has, upon written request, a right, enforceable in court, of access to federal agency records, unless such records (or portions thereof) are protected from disclosure by any of nine exemptions or three exclusions.

Headquarters

Census Bureau headquarters in Suitland, Maryland.

Information Security Incident

Any actual or suspected security incident that must be reported to the Bureau of Census Computer Incident Response Team (BOC CIRT). This can include mishandled information or threats to an IT systems and the Census Bureau network.

Malicious Code

A type of threat to information security. People write and transmit malicious code in an attempt to cause security breaches for unauthorized access to information, and to cause intentional damage to information system hardware and/or the information stored on the system.

Paradata

Auxiliary data collected during a sample survey, census, or other data collected that provides information about the data collection process.

Peer-to-Peer Applications

Instant messaging like Google Hangouts and Facebook chat, and file sharing programs like OneDrive, Dropbox, and BitTorrent.

Personally Identifiable Information (PII)

A type of information which may be either protected by law or administratively restricted, depending on what the information is and the context. PII refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. This could be a single item such as a name by itself, or information combined with other personal or identifying information which could be linked to a specific individual.

Phishing

The criminal attempt to acquire sensitive information such as user names, passwords and credit card information using electronic communications.

Physical Security

Includes procedures concerned with the way we protect our personnel, facilities, and property. The goal of physical security is to ensure the safety of Census Bureau personnel, information, computer resources, facilities, and other assets.

Privacy

An aspect of Data Stewardship that concerns respecting individuals' freedom from unauthorized and unwarranted intrusion into their personal information. Privacy relates

to the information we collect and how we collect it.

Privacy Act (Title 5 U.S.C. Section 552a)

The Privacy Act regulates Federal government agencies' collection, maintenance, use, and dissemination/disclosure of personal information. The purpose of the Act is to balance government agencies' need to maintain information about individuals with the rights of individuals to be protected against unwarranted/unauthorized access to or use of their personal information contained in files maintained by the Federal Government. In meeting its purpose, the Act restricts disclosure of personally identifiable records maintained by Federal agencies, subject to several narrow, stipulated exceptions; provides individuals increased rights of access to records about themselves maintained by Federal agencies; provides individuals rights to seek amendment of records about themselves maintained by Federal agencies; establishes a code of "fair information practices" requiring Federal agencies to comply with statutory norms for collection, maintenance, use, and dissemination/disclosure of personal information. Census data are NOT subject to these access and revision rights.

Under the Act, a Federal agency may not disclose a record pertaining to an individual without a written request or prior written consent from that individual unless the disclosure meets the terms of one or more of several stipulated exceptions. Exceptions allowing for disclosure include disclosure to agency employees who need the record in order to perform their duties; to another government agency within the United States for a civil or criminal law enforcement purpose (upon written request from that agency); in response to a court order; to the Census Bureau for planning or conducting a 13U.S.C. census, survey, or activity; or for a specified routine use. Census data may NOT be disclosed pursuant to any of the access provisions in the Act.

The Act provides criminal penalties for any unauthorized disclosure of agency records containing personal information. The Office of Management and Budget has general oversight responsibilities for implementation of the Act.

Privacy Impact Assessment (PIA)

An evaluation tool used to identify and mitigate privacy risks. PIA's are also an analysis instrument to help program or project managers consistently identify and evaluate privacy risks; and a means of sharing information with the public.

Protected Information

Protected information is information that is protected by laws such as Title 13 or Title 5. It can include information such as response data, address lists and frames, personnel data, and internal methodological data. It may include PII.

Public Information

Information that is released to a wide audience, such as statistical products, metadata, schedules, program descriptions, and risk plans, as well as information released under the Freedom of Information Act (FOIA).

Reimbursable Surveys

The Census Bureau, as a service to other agencies, conducts reimbursable surveys. These surveys may be conducted under Title 13 or Title 15. When they are conducted under Title 15, the data are confidential under the sponsoring agency's legislation and confidentiality requirements. If the survey is conducted under Title 13, then the restrictions of Title 13 confidentiality apply.

Restricted Access

A method of protecting Census Bureau data, that limits access, both electronic and physical, to those who have sworn to protect confidential data under Title 13 or Title 26 and who have a work-related need to know.

Security Audits

Routine checks of all technological safeguards to make sure they are working correctly.

Sensitive Information

Information that is either protected by law or administratively restricted. This is a “catchall” term that encompasses any information, the loss of, misuse of, or unauthorized access to, or modification of which could adversely affect the Census Bureau’s mission or operation and is subject to restriction by statute, regulation or policy directive. Sensitive information includes information provided by respondents or that could potentially identify a respondent. It also includes unpublished statistics or analytical reports whose release is time-sensitive or embargoed, is controlled by a contract, or whose purpose is for internal research or analysis. It may also include any administrative information employed to achieve the Census Bureau’s mission, including contracting, financial, budget, human resources, security, policy or legal materials such as opinions, advice and litigation documents. Because the term “Sensitive Information” is so broad, it is preferable to use it rarely, the better practice being to refer to the specific nature of the materials being discussed and the particular law, regulation or policy directive that is controlling.

Social Engineering

A type of activity that computer criminals use to manipulate and persuade people to reveal information that the criminal values. However, instead of software, social engineering works through lies, deceit, impersonation, and tricks.

Social Media

Webinars, blogs, social communities, wikis, and video or photo sharing sites.

Spam

Unsolicited e-mail messages.

Special Sworn Status (SSS)

Status conferred on non-Census Bureau individuals by the Census Bureau if these individuals need access to sensitive information to undertake a task that is necessary to perform work that supports the Census Bureau's mission. These individuals are not Census Bureau employees, but they are acting to assist the Census Bureau.

Spyware

Computer software that can threaten IT systems and resources. Spyware programs are designed to collect information from a user's computer without their informed consent. Also known as malware or privacy-invasive software.

Sworn Oath of Nondisclosure

Statement signed by Census Bureau employees and SSS individuals by which they enter into a life-long legal obligation to uphold the confidentiality provisions of Title 13 and acknowledge that they are subject to severe penalties for unlawful disclosure.

Technological Safeguards

Specific measures taken to ensure that computer systems protect data.

Telework Program/Telecommuting

Paid employment performed away from the regular office, at an alternate workplace. The Census Bureau's telework program enables headquarter employees to work effectively in a nontraditional setting. The telework program is open to all eligible

headquarters employees. Throughout the Washington capital region, telework programs have proven to offer both organizational and societal benefits, including reduced commuting time, positive environmental effects, and few interruptions.

Threat

An activity that has the potential to cause harm—whether deliberate or unintentional—to a system. Threats may include hackers, malicious code, and data entry errors. Threats exploit vulnerabilities.

Title 5

See Privacy Act.

Title 13

A federal law that, among other things, authorizes and directs the Census Bureau to conduct censuses and surveys and sets out the standards of confidentiality for the data collected. It imposes severe criminal penalties if these requirements are violated – up to \$250,000 in fines, up to 5 years in prison, or both. It also authorizes the Census Bureau to conduct surveys and provide statistical services for other federal agencies, state and local governments, and members of the private sector – subject to Title 13 confidentiality.

Title 15, Section 1525

A federal law that, among other things, permits the Secretary of Commerce to conduct special studies for other organizations. Under Title 15, identifiable data are returned to the sponsoring agency, because the data collected or acquired under the sponsoring agency's authority are subject to the sponsoring agency's legislation and confidentiality requirements – not Title 13.

Title 26

A federal law that, among other things, authorizes the Internal Revenue Service (IRS) to collect individual and business income taxes. It also provides the conditions under which the IRS may disclose Federal Tax Information (FTI) to other agencies. Specifically, it provides for the disclosure of FTI to the Census Bureau for statistical purposes in the structuring of censuses for conducting related statistical activities authorized by law. Title 26 also places specific requirements on the Census Bureau and other agencies to which IRS has disclosed data regarding the safeguarding of returns and return

information and authorizes severe criminal and civil penalties for any violations of these requirements.

Trojan Horse

A type of hostile computer program that contains malicious code masquerading as a valid software application. Trojan horse programs are often designed to trick users into copying and executing them.

Unauthorized Browsing

Unauthorized browsing is the act of searching or looking through protected data for other than work-related purposes.

Unauthorized Browsing Policy

Prohibits access to sensitive information for any reason other than work-related purposes, and it applies to all employees and Special Sworn Status individuals. That means even if you can access information legitimately (such as possessing active badge or system log-on), you must not access sensitive information unless you have a work-related need to do so.

Unlawful Disclosure

The act of allowing unauthorized access to information protected by the law. The laws may apply to your work in a variety of ways, depending on the situation.

Virtual Desktop Infrastructure (VDI)

VDI, or Virtual Desktop Infrastructure, is a means of expanding teleworker access to systems and data that is normally accessed when at work. Using a secure ID and password, the teleworker can connect to the Census Bureau's servers. Use of VDI allows teleworkers to access the same files as when physically at Census, including restricted information such as PII, Title 13, and Title 26 data.

Virus

Self-replicating computer code that operates and spreads by modifying or damaging executable files and data (i.e., files with a .exe extension). Viruses are most frequently transmitted through e-mail attachments. Viruses can also be transmitted by downloading malicious software (intentionally or unintentionally) from the Internet.

Vulnerability

A flaw or weakness that may allow another element to harm an information system. Vulnerabilities exist in hardware, software, and the environment in which the system resides.

Workstation

A desk-based computer connected to the Census Bureau computer system.

Worm

A computer programs that is self-contained, (i.e., code capable of operating without modifying any software) and is capable of spreading itself automatically. Cyber-criminals normally transmit worms by scanning a large number of systems for vulnerabilities.

**FY 2020 Data Stewardship and IT
Security Awareness Training (Text
Version)**

**CERTIFICATE
OF
COMPLETION**
=====

This Certificate Certifies

Print Full Name: _____
First Name Middle Name Last Name

Census Bureau Division: _____ Your Telephone Number: _____

Your Email Address: _____

Contractor Affiliation (if applicable): _____

Print Census COR or Census Supervisor's Name: _____
First Name Middle Name Last Name

has successfully completed the
**FY 2020 DATA STEWARDSHIP
AND IT SECURITY AWARENESS
TRAINING**

on

Completion Date

Employee/Contractor's Signature and Date

COR's Signature and Date (required for Contractors)

Note: To obtain credit for completing this training, please FAX this completion certificate to the
CIS OFFICE at 301-763-4158



No FEAR Act Training

1.1 Introduction

Welcome to the No FEAR Act Training. No FEAR Act means Notification and Federal Employee Anti-Discrimination and Retaliation Act. This mandatory training module for 2019- 2021 was prepared by the Department of Commerce, Office of Civil Rights. This training will familiarize you with the No FEAR Act and how it relates to you as a Commerce employee. Every employee must take No FEAR Act training within 90 days of appointment and on a following cycle of every two years.

At the conclusion of this training, you will know and understand the Basic Provisions of the No FEAR Act, anti-discrimination and whistleblower laws that protect you as a federal employee, your rights and the remedies available to you under these laws, and how to address alleged violations of anti-discrimination and whistleblower laws.

This training session should take about 40 minutes to complete.

To read along with the narration, please select the transcript button located at the top left corner of each slide.

If you need to leave this course before completion, please select the EXIT button to save your progress.

Let's begin!

1.2 No Fear Act Training Menu

This is the Notification and Federal Employee Anti-Discrimination and Retaliation Act Training Menu for the Department of Commerce. Starting with No FEAR Act Information, please select each button to learn about the No FEAR Act.

1.3 What is the No Fear Act?

Congress enacted the Notification and Federal Employee Anti-discrimination and Retaliation Act of 2002 (No FEAR Act) on May 15, 2002, and it became effective on October 1, 2003.

The No FEAR Act imposes additional duties upon federal agencies intended to make them more accountable for violations of anti-discrimination and whistleblower laws, and to reinvigorate their longstanding duty to provide a work environment free of discrimination and retaliation.

1.4 Federal Agency Requirements

The No FEAR Act requires each federal agency to do the following:

- ☐ Reimburse the U.S. Treasury's Judgment Fund for payments made for judgments and settlements of discrimination claims.
- ☐ Post statistical data to its website pertaining to EEO complaints.
- ☐ Submit an annual report to Congress, EEOC, the Department of Justice, and OPM detailing the status of complaints brought forth under anti-discrimination and whistleblower laws and its efforts to improve compliance with those laws.
- ☐ Provide annual notice to its employees, former employees, and applicants for employment concerning the rights and remedies applicable to them under employment discrimination and whistleblower protection laws; and
- ☐ Provide training, every two years, to its employees, including supervisors and managers, regarding the rights and remedies available under employment discrimination and whistleblower protections laws

1.5 Existing Rights Unchanged

According to Section 205 of the *No FEAR Act*, neither the act nor this notice creates, expands or reduces any rights otherwise available to any employee, former employee, or applicant under the laws of the United States, providing the provisions of law specified in 5 U.S.C. 2302(d).

1.6 Contract Employees

This training requirement DOES NOT extend to contract employees. However, overseas staff locally employed by the U.S. Foreign Commercial Service may take the *No FEAR Act* course. Issues raised by locally employed staff overseas should be handled at their Post and be consistent with their established procedures.

Select the No Fear Act Training Menu button to return to the training menu.

1.7 Discrimination Protection

As a federal employee, you are protected from discrimination in employment matters on the basis of your race, color, religion, sex, national origin, age, disability, parental status, sexual orientation, gender identity, marital status, political affiliation, and genetic information.

The laws forbid discrimination when it comes to any aspect of employment, including hiring, firing, pay, job assignment, promotion, layoff, training, fringe benefits, and any other term or condition of employment.

The following slide lists the anti-discrimination laws and the specific protections they provide.

1.8 Anti-Discrimination Laws

- ❑ Title VII of the Civil Rights Act of 1964, as amended, covers race, color, religion, national origin, sex, and retaliation
- ❑ The Pregnancy Discrimination Act of 1978, amended Title VII of the Civil Rights Act to prohibit sex discrimination on the basis of pregnancy
- ❑ The Equal Pay Act of 1963 covers sex-based pay differentials
- ❑ The Age Discrimination in Employment Act of 1967 covers individuals aged 40 and over
- ❑ The Rehabilitation Act of 1973, as amended, covers disability (physical and mental)
- ❑ The Americans with Disabilities Act Amendments Act of 2008 expands coverage of the Americans with Disabilities Act of 1990
- ❑ The Genetic Information Act of 2008 covers genetic information
- ❑ The Civil Service Reform Act of 1978 covers prohibited personnel practices

Select next to learn more about Title VII of the Civil Rights Act and the provisions it provides against anti-discrimination.

1.9 Title VII of the Civil Rights Act

Title VII of the Civil Rights Act prohibits employment discrimination based on race, color, religion, national origin, or sex.

This law also makes it illegal to retaliate against a person for participating in an EEO process or reasonably opposing conduct made unlawful by an EEO law.

Select the Title VII of the Civil Rights Act of 1964 button for more information.

Directions: Select each button to learn more about how Title VII of the Civil Rights Act helps with unlawful discrimination.

1.10 Unlawful Discrimination Based on Color

Title VII also prohibits discrimination based on color. There is no standard definition for the term "color," however, color has often been associated with race or a subgroup within a race.

Everyone, regardless of color, is a member of this protected class.

Select the Title VII of the Civil Rights Act of 1964 button to return to Title VII of the Civil Rights Act slide.

1.11 Unlawful Discrimination Based on Race

Race discrimination involves treating people unfavorably because they are of a certain race, or because of personal characteristics associated with race (such as hair texture, skin color, or certain facial features), or they are married to (or associated with) a person of a certain race or color.

It is unlawful for a federal agency to take an official action (for example, hiring, performance appraisal, promotion, award, discipline, termination, etc.) on the basis of race.

It is unlawful to harass a person because of his/her race or color. Unlawful harassment can include, for example, racial comments or conduct, offensive remarks, or the display of racially-offensive symbols.

Select the Race Discrimination button for more information.

Select the Title VII of the Civil Rights Act of 1964 button to return to Title VII of the Civil Rights Act slide.

1.12 Unlawful Discrimination Based on National Origin

National origin discrimination involves treating people unfavorably because they are from a particular country or part of the world; their ethnicity or accent; they appear to be of a certain ethnic background even if they are not; or they are married to (or associated with) a person of a certain national origin.

Discrimination can occur when the victim and the person who inflicted the discrimination are of the same national origin.

It is unlawful for a federal agency to take an official action (for example, hiring, performance appraisal, promotion, award, discipline, termination, etc.) on the basis of national origin.

It is unlawful to harass a person because of their national origin. Unlawful harassment can include, for example, offensive or derogatory remarks about a person's national origin, accent or ethnicity.

Select the National Origin Discrimination button for more information.

Select the Title VII of the Civil Rights Act of 1964 button to return to Title VII of the Civil Rights Act slide.

1.13 Unlawful Discrimination Based on Religion

Religious discrimination involves treating an applicant or employee unfavorably because of his or her religious beliefs or having no religious associations.

Religious discrimination can also involve treating someone differently because that person is married to or associated with an individual of a particular religion.

Agencies are required to reasonably accommodate an employee's religious beliefs or practices, unless doing so would cause more than a minimal burden on the operations of the employer's business. This means an employer may be required to make

reasonable accommodations to the work environment that will allow an employee to practice his or her religion. For example, approving leave for religious holidays falling on work days.

It is illegal to harass a person because of his or her religion. Unlawful harassment can include, for example, offensive remarks about a person's religious beliefs or practices.

Select the Religious Discrimination and Facts About Religious Discrimination buttons for more information.

Select the Title VII of the Civil Rights Act of 1964 button to return to Title VII of the Civil Rights Act slide.

1.14 Unlawful Discrimination Based on Sex (Gender)

Sex discrimination involves treating someone unfavorably because of that person's sex.

According to the EEOC, discrimination against an individual because of one's gender identity, transgender status, or sexual orientation is discrimination based on sex in violation of Title VII.

It is unlawful for a federal agency to take an official action (for example, hiring, performance appraisal, promotion, award, discipline, termination, etc.) on the basis of sex.

It is unlawful to harass a person because of that person's sex. Harassment can include "sexual harassment" or unwelcome sexual advances, requests for sexual favors, and other verbal or physical harassment of a sexual nature.

Harassment does not have to be of a sexual nature, however, it can include offensive remarks about a person's sex. For example, it is illegal to harass a woman by making offensive comments about women in general.

Both victim and the harasser can be either a woman or a man, and the victim and harasser can be the same sex.

Select the “What You Should Know About EEOC and the Enforcement Protections for LGBT Workers” and “Departmental Administrative Order 215-11-Complaint Process for Sexual Orientation Discrimination” buttons for more information.

Select the Title VII of the Civil Rights Act of 1964 button to return to Title VII of the Civil Rights Act slide.

1.15 Anti-discrimination Laws

There are additional laws that help protect against discrimination based on age, disability, genetic information, sex (gender), and reprisal or retaliation. Select each button to learn more about these anti-discrimination laws and the protections that are provided.

1.16 Unlawful Discrimination Based on Genetic Information

The Genetic Information Nondiscrimination Act of 2008 (GINA) states that it is illegal to discriminate against employees or applicants because of genetic information. The act prohibits the use of genetic information in making employment decisions; restricts employers from requesting, requiring or purchasing genetic information; strictly limits the exposure of genetic information; and, requires agencies to maintain the privacy of any genetic information acquired, with limited exceptions.

Select the Genetic Information Non-Discrimination Act (GINA) button for more information.

Select the Anti-Discrimination Laws button to return to the Anti-Discrimination Laws slide.

1.17 Unlawful Discrimination Based on Sex (Gender)

The Pregnancy Discrimination Act of 1978 amended Title VII to make it illegal to discriminate against a woman due to pregnancy, childbirth, or related medical conditions.

The Equal Pay Act of 1963 prohibits federal agencies from paying employees of one sex lower wages than those of the opposite sex for performing substantially equal work. Men and women in the same workplace must be given equal pay for equal work.

Select the Pregnancy Discrimination and The Equal Pay Act of 1963 buttons for more information.

Select the Anti-Discrimination Laws button to return to the Anti-Discrimination Laws slide.

1.18 Unlawful Discrimination Based on Reprisal or Retaliation

Federal agencies are prohibited from retaliating against an employee for activity involving equal employment opportunity. Retaliation (also known as reprisal) occurs when an adverse action is taken against an applicant or employee because he/she:

- ☐ Previously filed a complaint of discrimination
- ☐ Participated in a matter involving a complaint, to include giving evidence or testimony to an investigator or in a hearing, or
- ☐ Opposed any action that they perceived as discriminatory.

Select the Facts About Retaliation button for more information.

Select the Anti-Discrimination Laws button to return to the Anti-Discrimination Laws slide.

1.19 Unlawful Discrimination Based on Age

The Age Discrimination in Employment Act (ADEA) of 1967 prohibits discrimination against federal employees who are 40 years of age or older.

The act protects older employees from employment actions based on stereotypes or beliefs associated with age.

Select The Age Discrimination in Employment Act of 1967 button for more information.

Select the Anti-Discrimination Laws button to return to the Anti-Discrimination Laws slide.

1.20 Unlawful Discrimination Based on a Disability

The Rehabilitation Act of 1973, as revised, makes it illegal to discriminate against a qualified person with a disability in the federal government.

The law also requires agencies to provide reasonable accommodation to qualified employees and applicants with disabilities, unless to do so would cause undue hardship.

Although the Rehabilitation Act applies to Federal employees, recent changes under the act have made its protections the same as those provided under the Americans with Disabilities Act Amendments Act of 2008 (ADAAA).

Select the Disability Discrimination button for more information.

Select next to learn more about individuals with disabilities.

1.21 Definition of an Individual with a Disability

The Americans with Disabilities Act Amendment Act of 2008, revised the Americans with Disabilities Act of 1990, to broaden the scope of protection and expand the definition of

the term “disability” making it easier for individuals with disabilities to be covered under the law.

Under the ADAAA, a person is considered an individual with a disability if he/she:

- ☐ Has a physical and/or mental impairment that substantially limits one or more major life activities (for example, breathing, walking, seeing, hearing, or performing manual tasks.)
- ☐ Has a record or past history of physical and/or mental impairment that substantially limited a major life activity.
- ☐ Is regarded by the agency as having a physical and/or mental impairment and an action, prohibited by law, is taken because of an actual or perceived impairment that is not temporary or minor.

Select the Disability Discrimination button for more information.

Select next to learn about accommodating individuals with disabilities.

1.22 Reasonable Accommodation

The federal government has a duty to provide a reasonable accommodation to “qualified” individuals with disabilities, who are employees or applicants for employment, unless to do so would cause an undue hardship (significant difficulty or expense).

A reasonable accommodation is a modification or adjustment to the application process, work environment, or change in the way the job is customarily done, to enable a person with a disability to perform the essential functions of the position or to enjoy

equal benefits and privileges of employment, as are enjoyed by other similarly situated employees without disabilities.

The accommodation does not have to be exactly what is requested by the employee, but must be reasonable and effective.

The agency does not have to change performance standards or eliminate essential duties of your position as a reasonable accommodation.

Select the Enforcement Guidance button for more information.

Select the Anti-discrimination laws button to return to the Anti-discrimination Laws slide.

1.23 Additional Protections Against Unlawful Discrimination

The Civil Service Reform Act of 1978 requires fair and equitable treatment for employees and applicants seeking employment in all aspects of personnel management without regard to their race, color, religion, national origin, sex, age, disability, and also political affiliation or marital status.

Select the Civil Service Reform Act of 1978 button for more information.

Additionally, Presidential Executive Orders prohibits discrimination on the basis of sexual orientation and status as a parent.

Select the Executive Order 13087 button for more information.

1.24 Secretarial Policy Statement

The Department of Commerce prohibits discrimination based on race, color, religion, sex (including sexual harassment and pregnancy discrimination), sexual orientation,

gender identity, national origin, age (40 years of age and over), genetic information, or disability (physical or mental).

Retaliation is also strictly prohibited.

Select the Secretarial Policy Statement button for more information.

Select the No Fear Act Training Menu button to return to the training menu.

1.25 Employee Rights Under EEO

Employees rights under EEO:

- ☐ You have the right to be offered an opportunity to use the Agency's Alternative Dispute Resolution program to resolve your workplace conflict or dispute.
- ☐ You have the right to a representative of your choice. However, your representative's role cannot conflict with his/her official duties with the organization. The right to representation applies throughout the complaint process, including the counseling stage and during mediation.
- ☐ You have the right to confidentiality of all discussions in mediation.
- ☐ Prior to filing a formal complaint, you have a right to remain anonymous.

1.26 Employee Rights Under EEO (2)

Where counseling is selected and the dispute has not been resolved, you have a right to receive, in writing, *within 30 calendar days of the first counseling contact (unless you agree in writing to an extension)*, a notice terminating counseling and informing you of:

- ☐ The right to file a formal individual or class complaint within 15 calendar days of receipt of the notice.

☐ The appropriate official with whom to file a formal complaint.

☐ Your duty to immediately inform the agency if you retain counsel or a representative.

1.27 Employee Rights Under EEO (3)

☐ Where ADR is selected and the dispute has not been resolved, you have a right to receive in writing, the notice terminating counseling, upon completion of the mediation or within ninety (90) calendar days of the first contact with the EEO Counselor, whichever is earlier.

☐ You have the right to pursue formal complaint processing, including administrative and court action, should you wish to discontinue the mediation process or are unable to reach a settlement through ADR (if ADR was selected.)

☐ You have a right to go directly to a court of competent jurisdiction on claims of sex-based wage discrimination under the Equal Pay Act even though such claims can also be brought under Title VII of the Civil Rights Act.

☐ In age discrimination claims raised under ADEA, as an alternative to the EEO administrative process, you have a right to file a civil action in Federal District Court upon providing 30 days advanced notice to the Equal Employment Opportunity Commission.

1.28 Employee Rights Under EEO (4)

☐ You have a right to request a hearing before an EEOC Administrative Judge (except in a mixed case involving actions appealable to the Merit Systems Protection Board) after completion of the investigation or 180 calendar days from the filing of a formal complaint, whichever comes first.

☐ You have a right to an immediate final decision after an investigation by the agency in accordance with 29 C.F.R. §1614.108(f).

☐ You have a right to go to U.S. District Court 180 calendar days after filing a formal complaint if no final action has been taken on the complaint, or 180 days after filing an appeal if no decision has been issued on the appeal.

Select next to learn about the remedies available to employees under EEO.

1.29 Remedies Available to Employees Under EEO

Whenever discrimination is found, the goal of the law is to put the victim of discrimination in the same position, or nearly the same, that he or she would have been if the discrimination had never occurred.

The types of relief will depend upon the discriminatory action and the effect it had on the victim. For example, if someone is not selected for a job or promotion because of discrimination, the remedy may include placement in the job and/or back pay and benefits the person would have received.

Starting with Compensatory Damages, select each button to learn about damages due to discrimination.

Compensatory Damages:

For cases involving intentional discrimination based on a person's race, color, national origin, sex (including pregnancy, gender identity, and sexual orientation), religion, disability, or genetic information.

Compensatory Damages:

Compensatory damages pay victims for out of pocket expenses caused by the discrimination and any emotional harm suffered.

☐ Compensatory Damages are capped at \$300,000

☐ A victim of discrimination may also be able to recover **attorney's fees, expert witness fees, and court costs.**

Sex Discrimination & Liquidated Damages:

In cases involving intentional sex-based wage discrimination under the Equal Pay Act, victims cannot recover compensatory damages, but may be entitled to "liquidated damages."

The amount of liquidated damages that may be awarded is equal to the amount of back pay awarded to the victim.

Select the Additional Information button for more information.

Select the No Fear Act Training Menu button to return to the training menu.

1.30 Addressing Prohibited Employment Discrimination Outside of the EEO Process

Claims of sexual orientation discrimination, status as a parent, political connection, and marital status discrimination may be addressed through different processes.

At Commerce, employees and applicants for employment may also file complaints involving sexual orientation discrimination with the EEO Office.

Select the Processing Complaints of Discrimination by LGBT Federal Employees button for more information.

Applicants and employees may also use the resources below to address discrimination claims that are also covered outside of the EEO process.

Select the Prohibited Personnel Practices and U.S. Merit Systems Protections Board buttons for more information.

Select the No Fear Act Training Menu button to return to the training menu.

1.31 Addressing Alleged Discrimination through the EEO Process

You must contact an EEO counselor within 45 calendar days of the date of the matter suspected to be discriminatory or, in the case of a personnel action, within 45 calendar days of the effective date of the action, or when you first became aware of the suspected discrimination.

The names and telephone numbers of EEO counselors are available on bulletin boards, Internet websites, or by contacting your EEO Officer listed on Commerce's Office of Civil Rights website.

Select the EEO Officers and EEO Complaint Process buttons for more information.

1.32 Contacting an EEO Counselor

Once you contact an EEO counselor, the EEO Counselor will try to resolve the issue through EEO counseling or offer an opportunity to use the Alternative Dispute Resolution (ADR) process.

If the issue is not resolved, you will be provided a Notice of Right to File a Formal Complaint. You must file a formal complaint within 15 calendar days from receipt of the notice.

Employees covered by a negotiated bargaining agreement, which addresses claims of discrimination, may elect to proceed under the negotiated bargaining agreement, rather than filing a formal complaint of discrimination.

You cannot do both.

Select the No Fear Act Training Menu button to return to the training menu.

1.33 Whistleblower Protection Laws

The Whistleblower Protection Act (WPA) of 1989 was signed into law to strengthen protections for federal whistleblowers. The WPA states that whistleblowers serve the public interest by assisting in the removal of fraud, waste, abuse, and unnecessary government expenditures.

Starting with “Who is a Whistleblower?,” select each button for answers to the questions.

Who is a Whistleblower?

A whistleblower is a government employee, former employee, or applicant for employment who makes a protected disclosure.

While NOAA Corps Officers do not have statutory coverage under the Whistleblower Protection Act, they have been extended protection from retaliation as a matter of Departmental policy.

Select the OIG Publication button for more information.

What is a Protected Disclosure?

A Protected Disclosure is anything you report and reasonably believe to show:

- ☐ A violation of law, rule, or regulations;
- ☐ Gross mismanagement/gross waste of funds;
- ☐ Abuse of authority
- ☐ A substantial and specific danger to public health or safety

Any federal employee who reasonably believes the information being disclosed shows one of the conditions above may be a whistleblower.

Select the No Fear Act Training Menu button to return to the training menu.

1.34 Employee Reporting Responsibilities

It is the responsibility of every employee to report suspected wrongdoing, including, but not limited to: waste, fraud, loss, unauthorized use, abuse, or mismanagement of federal funds, property, and assets. It is also the responsibility of every employee to fully cooperate with any Office of the Inspector General (OIG) audit, inspection, evaluation, or investigation.

DOC managers must escalate reports of suspected wrongdoing involving fraud, waste, and abuse; fully cooperate and support the OIG investigations to promote and ensure quick and timely resolution of any wrongdoing.

We accomplish this great mission of service and stewardship by supporting and nurturing DOC's culture of integrity and accountability.

Select the No Fear Act Training Menu button to return to the training menu.

1.35 EEO Contact Information

Bureau EEO Offices

📞 Census Bureau (CB): 301-763-2853 or 800-872-6096

📞 National Processing Center: 812-218-3472

📞 National Institute of Standards and Technology (NIST): 301-975-2038

📞 National Oceanic Atmospheric Administration (NOAA): 301-713-0500

☞ US Patent and Trademark Office (USPTO): 571-272-8292

The EEO Office for the Office of Secretary (202-482-8121) is responsible for the following bureaus:

☞ Bureau of Economic Analysis (BEA)

☞ Bureau of Industry and Security (BIS)

☞ Economic Development Administration (EDA)

☞ International Trade Administration (ITA)

☞ Minority Business Development Agency (MBDA)

☞ National Telecommunications and Information Administration (NTIA)

☞ National Technical Information Service (NTIS)

☞ Office of General Counsel (OGC)

☞ Office of Inspector General (OIG)

☞ Office of the Chief Information Officer (OCIO)

☞ First Responder Network (FirstNet)

☞ Denali Commission

1.36 Other Resources

The Office of Civil Rights created a chart to provide Department of Commerce employees and managers with a quick reference to resources for addressing employment-related issues, concerns, and/or disputes.

The chart can be found by selecting the Addressing Workplace Issues at a Glance button.

Select the No Fear Act Training Menu button to return to the training menu.

1.37 How to Report Whistleblowing Activities

An employee may report wrongdoing, or whistleblow, through the following channels:

- ☐ Report to the DOC Office of Inspector General (OIG) Hotline by phone, fax, or web form
- ☐ Report to the Office of Special Counsel (OSC), an independent federal agency that investigates prohibited personnel practices, especially whistleblower retaliation claims
- ☐ Report to a supervisor in their chain of command

NOTE: For whistleblower disclosures involving classified national security information or other information protected from public release by law (for example, patient privacy information), whistleblowers must use confidential channels such as OIG, OSC, or Congress in order to be protected from adverse personnel actions related to their disclosures.

Select each button to learn the whistleblowing channels.

Select the No Fear Act Training Menu button to return to the No Fear Act Training Menu.

1.38 OIG Reporting Avenues

Reporting suspected discrimination concerning DOC programs and operations to OIG, including those financial in nature, is an easy process and can be done confidentially or anonymously.

Select the Report Fraud, Waste, Abuse, & Whistleblower Reprisal button for more information.

Select the Online Hotline Complaint Form button to submit a hotline complaint form.

Select the How to Report Whistleblowing Activities button to return to the How to Report Whistleblowing Activities slide.

1.39 Reporting Whistleblower Retaliation Claims

Any employee or applicant who believes he or she has been retaliated against because of protected whistleblowing, may file a complaint with the Office of Special Counsel (OSC). The complaint must be in writing, and you must use a standardized complaint form. Select the Complaint Dashboard button for more information.

A whistleblower does not need an attorney to file a complaint.

OSC is an independent federal agency with authority to investigate and seek corrective action in cases of whistleblowing retaliation. OSC may also bring disciplinary charges against officials who retaliate against whistleblowers.

1.40 Reporting Whistleblower Retaliation Claims

Every employee has a duty to maintain the highest standards of integrity in government.

In order to ensure that the highest standards are maintained, each agency has an OIG that also receives disclosures. Upon the employee's request, the OIG will protect the identity of the individual whistleblower, unless the OIG determines that disclosure is unavoidable in the course of the investigation.

Select the How to Report Whistleblowing Activities button to return to the How to Report Whistleblowing Activities slide.

1.41 Reporting to a supervisor

Any employee or applicant who believes he or she has been retaliated against because of protected whistleblowing may notify a supervisor in their chain of command.

Select the How to Report Whistleblowing Activities button to return to the How to Report Whistleblowing Activities slide.

1.42 Remedies for Retaliation Against Whistleblowers

Employees' remedies for retaliation can include:

- ☐ Corrective action, such as reinstatement or overturning a job action and back pay, and
- ☐ Damages, including attorney's fees, medical, travel costs, and compensatory damages

Consequences for supervisors found to have engaged in retaliation may include disciplinary action sought by the Office of Special Counsel or the agency. This can include removal, reduction in grade, suspension, reprimand, exclusion, and/or civil penalty up to \$1,000 (5 U.S.C. § 1215).

Select the No Fear Act Training Menu button to return to the training menu.

1.43 Management Responsibilities for EEO

Managers and supervisors are required to:

Provide a reasonable amount of official time for employees to work on an EEO complaint.

Cooperate with an EEO counselor or EEO investigator. Failure to do so may result in disciplinary action.

Ensure employees are not subjected to a hostile work environment.

Ensure employees are not retaliated against for EEO activity

Ensure legitimate, non-discriminatory reason for all employment actions.

Ensure employees are treated fairly and equally.

Ensure prompt and effective action to address claims of harassment by referring to DAO 202-955.

Provide reasonable accommodation to a qualified individual with a disability.

Provide reasonable accommodation for religious beliefs and practices.

Disclose medical information only to officials with a need to know and keep medical information separate from personnel files.

Select the No Fear Act Training Menu button to return to the training menu.

1.44 Whistleblower Protection

For whistleblower contact information visit OIG.doc.gov or go to the OSC website at OSC.gov.

Select the No Fear Act Training Menu button to return to the training menu

1.45 Conclusion

Congratulations! You have just completed this module. You now know more about the No FEAR Act and the protections they provide.

Please select the Exit button to receive course credit.

This Page Intentionally Left Blank